On the use of the discrete power function for building public-key cryptosystems

BOGDAN GROZA
Department of Automatics and Applied Informatics
University Politehnica Timisoara
Bd. Vasile Parvan nr. 2, Room A304, 300223, Timisoara, Romania
ROMANIA
http://www.aut.upt.ro/~bgroza

Abstract: - This paper proposes a generalization of the discrete power function that can be used for constructing public-key cryptosystems. Particular cases of this function, with specific values for the encryption exponent, are used in RSA and Rabin cryptosystem. This paper provides a cryptosystem that can be built on a generalization of this function that holds for any value of the encryption exponent.

Key-Words: - cryptography, public key cryptosystem, one-way trapdoor function, discrete power function, trapdoor permutation.

1 Introduction

The discovery of public-key cryptosystems was a great turn in the history of cryptology [5]. These cryptosystems are vital to the security of information exchange and building public-key cryptosystems is an important subject. In order to construct such cryptosystems trapdoor one-way functions are needed, therefore finding such functions is itself a goal.

Different trapdoor one-way function based on the difficulty of the integer factorization problem can be found in literature and the first proposals were the RSA and Rabin cryptosystems [10], [11]. Also in the last decade new candidates were proposed [7], [8], [9].

In present days, in order to increase the security of public key cryptosystems, padding techniques, such as the well known RSA-OAEP [2], are used. Also, in order to increase efficiency, public key encryption schemes can be integrated in more complex frameworks for hybrid encryption, such as the KEM/DEM (key encapsulation mechanism, data encryption mechanism) from [4] or the Tag KEM/DEM from [1], in which public key encryption is used to securely exchange a secret key that is used to encrypt a message using symmetric techniques.

The contribution of this paper consists in proposing the general case of the discrete power function for constructing public key cryptosystems.

The paper is organized as follows. In section 2 some definitions and notations are introduced and two classical cryptosystems based on the integer factorization problem are recalled (Rabin and RSA). In section 3 a public key encryption scheme based on the generalization of the discrete power function is introduced. Section 4 holds the conclusions of the paper.

2 Related public key cryptosystems

2.1. Some notations and definitions

In order to simplify the exposition, in this section we recall some notations and definitions.

Definition 1 (PKE). A public key encryption scheme PKE consists in the following three algorithms $\{PKE.Gen(1^k), PKE.Enc(m,PK), PKE.Dec(c,SK)\}$ such that:

- $PKE.Gen(1^k)$: is a probabilistic polynomial time algorithm that on input $1^k, k \in Z_{x>0}$ outputs a public key, secret key pair (PK,SK), i.e. $(PK,SK) \leftarrow PKE.Gen(1^k)$.
- $PKE.Enc(m,PK)$: is a probabilistic polynomial time algorithm that takes as input a message m from the plaintext space, a public key PK and outputs the ciphertext c, i.e. $c \leftarrow PKE.Enc(m,PK)$.
- $PKE.Dec(c,SK)$: is a probabilistic polynomial time algorithm that takes as input a ciphertext c, a secret key SK and outputs a

message m, i.e. $m \leftarrow PKE.Dec(c, SK)$.

We also require that for any key pair $(PK, SK) \leftarrow PKE.Gen(1^k)$ and for any message m it holds $m \leftarrow PKE.Dec(PKE.Enc(m, PK), SK)$. This means that the public-key encryption is sound and the decryption of the encryption of a message always returns the original message.

Definition 2 (The discrete power function). We define the discrete power function as:

$$f : Z_n^* \to Z_n^*$$
$$f(x) = x^{\varepsilon} \bmod n \qquad (1)$$

Here Z_n^* denotes the multiplicative group of Z_n which is the set of integers from $Z_n = \{0,1,...,n-1\}$ that are relatively primes to n, i.e. $Z_n^* = \{x \in Z_n \mid \gcd(x,n) = 1\}$, and ε is an integer exponent (different cases according to the values of this exponent are to be treated in the following sections). The order of the multiplicative group of Z_n, i.e. Z_n^*, is given by the Euler phi function $\phi(n)$ which can be computed if and only if the factorization of n is known. Since exponents can be reduced modulo the order of the group, i.e. $x^{\varepsilon} \equiv x^{\varepsilon \bmod \phi(n)} \bmod n$, we assume that $1 < \varepsilon < \phi(n)$.

Less rigorous, but sufficient for an intuitive definition, a one-way function and a trapdoor one-way function are defined as follows.

Definition 3 (One-way function). A function $f : A \to B$ is said to be one-way if given $x \in A$ it is easy to compute $f(x)$ but given $y \in \mathrm{Im}(f)$ it is infeasible to compute $x \in A$ such that $f(x) = y$.

Definition 4 (Trapdoor One-way function). A function $f : A \to B$ is said to be trapdoor one-way if function f is a one-way function and there exists an information called trapdoor such that given $y \in \mathrm{Im}(f)$ it is easy to compute $x \in A$ such that $f(x) = y$.

Additionally, if function f is also bijective then it is called a trapdoor one-way permutation.

2.2. The RSA and Rabin cryptosystems

The RSA and Rabin cryptosystems [10], [11] are the first public key cryptosystems constructed on the discrete power function and their security relies on the intractability of the integer factorization problem. They both use a particular case of the discrete power function as follows:

$$f_{RSA} : Z_n^* \to Z_n^*$$
$$f_{RSA}(x) = x^{\varepsilon} \bmod n, \gcd(\varepsilon, \phi(n)) = 1 \qquad (2)$$

$$f_{Rabin} : Z_n^* \to Q_n$$
$$f_{Rabin}(x) = x^2 \bmod n \qquad (3)$$

Here Q_n denotes the set of quadratic residues from Z_n^*, i.e. $Q_n = \{x \in Z_n^* \mid \exists y \in Z_n^*, x = y^2 \bmod n\}$.

It is important to note that Rabin function is not a particular case of the RSA function since the RSA function requests that $\gcd(\varepsilon, \phi(n)) = 1$ and this does not hold in the case when the exponent is $\varepsilon = 2$ since $\phi(n)$ is always even. This leads to the following relevant difference between these two cryptosystems: RSA function is bijective, therefore it is a trapdoor one-way permutation, while Rabin function is not bijective. In the case when the integer n is a product of two distinct primes Rabin function is a 4 to 1 map, which means that each ciphertext computed with this function, which is a quadratic residue, has exactly 4 different plaintexts that correspond to it, i.e. 4 square roots, and choosing the correct one is possible if some redundancy is used.

In the particular case when n is a Blum integer, i.e. $n = p \cdot q$ and $p \equiv q \equiv 3 \bmod 4$, only one of the roots of each quadratic residue is also a quadratic residue. In this case the Rabin function defined on the set of quadratic residues, i.e. $f_{Rabin} : Q_n \to Q_n$, becomes a trapdoor one-way permutation.

What is probably more relevant in the difference between Rabin and RSA cryptosystems is that the security of Rabin cryptosystem is proved to be equivalent to factoring, it is commonly known that if one can compute square roots in Z_n^* then it can also factor n since if x and y are square roots of the same number and $x \neq \pm y \bmod n$ then $\gcd(x - y, n)$ gives a non-trivial factor of n. Still, a proof about the equivalence of RSA to factoring does not exists, and more, recently, there is some skepticism that such a proof exists [3].

More recent proposals of trapdoor one-way functions based on the intractability of integer factorization can be found in [7], [8], [9].

3. A public key encryption scheme for the general case of the discrete power function

Now we want to extend the use of the discrete power function (1) in public key cryptosystems for the remaining cases when the exponent is not relatively prime to the order of the group, i.e. $\gcd(\phi(n),\varepsilon)\neq 1$. Finally, this extension generalizes the use of this function for any kind of exponent prime or not to the order of the group, i.e. $\gcd(\phi(n),\varepsilon)\geq 1$.

We proceed by observing that in this case there exists a number τ such that the following relation holds:

$$\gcd\left(\frac{\phi(n)}{\gcd(\phi(n),\varepsilon^{\tau})},\varepsilon\right)=1 \qquad (4)$$

Let $\tau_{\min}$ be the minimal value of τ for which relation (4) holds. Now we define:

$$\phi'(n)=\frac{\phi(n)}{\gcd(\phi(n),\varepsilon^{\tau_{\min}})} \qquad (5)$$

Since now ε is prime to $\phi'(n)$ it means that ε has a multiplicative inverse in $Z_{\phi'(n)}$. Let this inverse be δ' such that $\delta'\cdot\varepsilon\equiv 1\bmod\phi'(n)$. Now we define the following function:

$$g(x)=x^{\delta'}\bmod n \qquad (6)$$

Now we claim the following:

Theorem 1. For f, g defined by (1), (6) it holds that $g\left(f^{\tau_{\min}+1}(x)\right)=f^{\tau_{\min}}(x)$. Here $f^{\tau_{\min}}(x)$ denotes the successive composition of f with herself for $\tau_{\min}$ times, i.e. $f^{\tau_{\min}}(x)=\underbrace{f\left(f\left(\ldots f(x)\ldots\right)\right)}_{\tau_{\min}}$.

Proof. From relation (6) we have $g\left(f^{\tau_{\min}+1}(x)\right)=x^{\varepsilon^{\tau_{\min}+1}\delta'}\bmod n=x^{\varepsilon^{\tau_{\min}}\varepsilon\delta'}\bmod n$, but, since $\varepsilon\delta'\equiv 1\bmod\phi'(n)\Leftrightarrow\varepsilon\delta'=1+k\phi'(n)$ for some integer k, it follows that $g\left(f^{\tau_{\min}+1}(x)\right)=x^{\varepsilon^{\tau_{\min}}(1+k\phi'(n))}\bmod n=x^{\varepsilon^{\tau_{\min}}+\varepsilon^{\tau_{\min}}k\phi'(n)}\bmod n$. Now from relation (5) it is trivial to deduce that $\varepsilon^{\tau_{\min}}\phi'(n)=j\phi(n)$ for some integer j and this obviously leads to $x^{k\varepsilon^{\tau_{\min}}\phi'(n)}\equiv 1\bmod n$ which let us conclude that $g\left(f^{\tau_{\min}+1}(x)\right)=x^{\varepsilon^{\tau_{\min}}}\bmod n=f^{\tau_{\min}}(x)$.

It is also straight forward to extend the result from theorem 1 for any $\tau>\tau_{\min}$, in this case it holds that $g\left(f^{\tau+1}(x)\right)=f^{\tau}(x),\forall\tau>\tau_{\min}$ and this can be proved in a similar manner.

The result from theorem 1 addresses the general case of the discrete power function and this case holds for any value of the exponent ε (prime or not to the order of the group). From this result it is easy to build a public key cryptosystem based on the general case of the discrete power function. By following the formalism from definition 1 we obtain the following cryptosystem:

- $PKE.Gen\left(1^{k}\right)$: Choose at random two distinct k bit primes p and q (here k is a security parameter). Compute: $n=pq$, $\phi(n)=(p-1)(q-1)$, $n=pq$. Choose an integer exponent ε then compute $\tau_{\min}$, $\phi'(n)$ as shown in relations (1), (2) and δ' as the multiplicative inverse of ε in $Z_{\phi'(n)}$, i.e. $\delta'\cdot\varepsilon\equiv 1\bmod\phi'(n)$. Return (PK,SK) where: $PK=(n,\varepsilon,\tau_{\min})$, $SK=(n,\delta')$.
- $PKE.Enc(m,PK)$: Choose a random integer r and compute $c_1=f^{\tau_{\min}+1}(r)=r^{\varepsilon^{\tau_{\min}+1}}\bmod n$ and $c_2=f^{\tau_{\min}}(r)\cdot m\bmod n=r^{\varepsilon^{\tau_{\min}}}\cdot m\bmod n$. Return the ciphertext $c\leftarrow(c_1,c_2)$.
- $PKE.Dec(c,SK)$: Compute the value of $m=\left(c_1^{\delta'}\right)^{-1}\cdot c_2\bmod n$. Return the message m.

Proving that decryption works is a straight forward consequence of theorem 1, obviously $c_1^{\delta'}=g\left(f^{\tau_{\min}+1}(r)\right)=r^{\varepsilon^{\tau_{\min}}}\bmod n$ from which follows that $m=\left(c_1^{\delta'}\right)^{-1}\cdot c_2\bmod n$.

It may be relevant to note that in fact this cryptosystem uses the discrete power function in order to exchange a key encrypted in c_1 and use this key to encrypt the actual message in c_2. This approach is related to the ElGamal cryptosystem [6] although here the inversion of the one-way function is based on the integer factorization problem.

The introduced cryptosystem is more efficient as the value of $\tau_{\min}$ is smaller since it may be expensive to iterate function f for $\tau_{\min}+1$ times. Therefore the most efficient case is when $\tau_{\min}=0$

which requires $\gcd(\phi(n),\varepsilon)=1$, this is in fact the case of the RSA function. In this case, since the function is a one-way trapdoor permutation, there is no reason to exchange a random key and one can directly encrypt the message as in the RSA cryptosystem - therefore in this case using directly the RSA cryptosystem is more efficient.

In order to simplify the description of the previous cryptosystem we consider giving a description of the cryptosystem for a small value of $\tau_{\min}$ which makes encryption faster. For example we take $\tau_{\min}=2$:

- $PKE.Gen(1^k)$: Choose at random two distinct k bit primes p and q. Compute: $n=pq$, $\phi(n)=(p-1)(q-1)$, $n=pq$. Choose an integer exponent ε such that $\gcd(\phi(n),\varepsilon)\neq 1$ and $\gcd\left(\frac{\phi(n)}{\gcd(\phi(n),\varepsilon^2)},\varepsilon\right)=1$. Compute $\phi'(n)=\frac{\phi(n)}{\gcd(\phi(n),\varepsilon^2)}$ and $\delta'=\varepsilon^{-1}\bmod\phi'(n)$. Return (PK,SK) where: $PK=(n,\varepsilon)$, $SK=(n,\delta')$.
- $PKE.Enc(m,PK)$: Choose a random integer r and the compute the ciphertext $c_1=r^{\varepsilon^3}\bmod n$ then the ciphertext $c_2=x^{\varepsilon^2}\cdot m\bmod n$. Return the ciphertext $c\leftarrow(c_1,c_2)$.
- $PKE.Dec(c,SK)$: Compute the value of $m=\left(c_1^{\delta'}\right)^{-1}\cdot c_2\bmod n$. Return the message m.

It may be relevant to note that the condition $\tau=2$ is also satisfied by the Rabin cryptosystem in the case when the modulus is a Blum integer.

It is also interesting to investigate when the general case of the discrete power function can be turned into a trapdoor one-way permutation. The following theorem shows how this can be achieved by making a restriction on its input domain.

Theorem 2. Let f be the discrete power function and g the function from (6) define $Z_n^\tau=\left\{x\in Z_n^*\middle|\exists\lambda,\alpha,\lambda>\tau,\alpha\in Z_n^*, f^\lambda(\alpha)=x\right\}$ then $f:Z_n^\tau\to Z_n^\tau$ is a trapdoor permutation and g is its inverse.

Proof. Theorem 2 can proved in a similar manner to theorem 1. We prove that for any $x\in Z_n^\tau$ it holds that $g(f(x))=x$. Obviously $g(f(x))=x^{\varepsilon\delta'}\bmod n$ and since $x\in Z_n^\tau$ we have $x=\alpha^{\varepsilon^\lambda}\bmod n$ for some α,λ. This means that $x^{\varepsilon\delta'}\equiv\alpha^{\varepsilon^{\lambda+1}\delta'}\bmod n\equiv\alpha^{\varepsilon^\lambda\varepsilon\delta'}\bmod n\equiv\alpha^{\varepsilon^\lambda(1+k\phi')}\bmod n$ and since $k\varepsilon^\lambda\phi'(n)$ is a multiple of $\phi(n)$ it leads to $x^{\varepsilon\delta'}\equiv\alpha^{\varepsilon^\lambda}\equiv x\bmod n$ and this proves theorem 2.

Therefore, if one can choose messages as integers from Z_n^τ then this function can be used as a trapdoor permutation to encrypt them. However we do not see any elegant way to perform this, and therefore the previously constructed cryptosystems remains the only efficient construction.

However, for the completeness of the result we want now to establish the number of elements from Z_n^τ. The following theorem gives a result that can be used for this purpose.

Theorem 3. Let e be some integer exponent, the number of e^{th} residues, i.e. numbers that can be written as $x^e\bmod n$, in Z_n^* is $\frac{(p-1)\cdot(q-1)}{\gcd(e,p-1)\cdot\gcd(e,q-1)}$.

Proof. In order to prove this we first want to establish the number of e^{th} residues in Z_p^* where p is a prime number. We claim that the number of e^{th} residues in Z_p^* is $\frac{p-1}{\gcd(e,p-1)}$. Let $g=\gcd(e,p-1)$. Since p is prime Z_p^* has generators. Now let α be a generator of Z_p^*, obviously some number x is an e^{th} residue if and only if it can be written as $\alpha^{e\cdot i}\bmod p$. Also, since α is a generator of Z_p^*, we have $\alpha^{e\cdot i}\equiv\alpha^{e\cdot j}\bmod p$ if and only if $i\cdot e\equiv j\cdot e\bmod(p-1)$. This can be also written as $i\cdot g\cdot\frac{e}{g}\equiv j\cdot g\cdot\frac{e}{g}\bmod g\frac{p-1}{g}$ and holds if and only if $i\cdot\frac{e}{g}\equiv j\cdot\frac{e}{g}\bmod\frac{p-1}{g}$. But $\gcd\left(\frac{e}{g},\frac{p-1}{g}\right)=1$ and therefore there exists $\left(\frac{e}{g}\right)^{-1}$ by which the previous relation can be multiplied leading to $i\equiv j\bmod\frac{p-1}{g}$. This leads to the fact that if and only if $i\neq j\bmod\frac{p-1}{g}$ we have $\alpha^{e\cdot i}\neq\alpha^{e\cdot j}\bmod p$ and therefore the number of e^{th}

residues in Z_p^* is $\frac{p-1}{\gcd(e, p-1)}$ (since there are $\frac{p-1}{\mathrm{g}}$ distinct elements in $Z_{\frac{p-1}{\mathrm{g}}}$).

As the number of e^{th} residues in Z_p^* is established it is straight forward to establish the number of e^{th} residues in Z_n^*. Because of the isomorphism between Z_n^* and $Z_p^* \times Z_q^*$ (this isomorphism is defined by the Chinese remainder theorem which is a basic fact in number theory and since it is commonly known we will not state it in this paper) it follows that the number of e^{th} residues in Z_n^* is $\frac{(p-1)\cdot(q-1)}{\gcd(e, p-1)\cdot\gcd(e, q-1)}$.

Now, by replacing the value of e with ε^τ, we obtain $\left|Z_n^\tau\right| = \frac{(p-1)\cdot(q-1)}{\gcd(\varepsilon^\tau, p-1)\cdot\gcd(\varepsilon^\tau, q-1)}$. Since the elements of Z_n^τ are uniformly distributed the probability that a random element $0 \le r < n$ is in Z_n^τ is $\frac{\left|Z_n^\tau\right|}{n}$. This probability is high only if the value of $\gcd(\varepsilon^\tau, p-1)\cdot\gcd(\varepsilon^\tau, q-1)$ is small and in this case choosing at random a value that is in Z_n^τ can happen with high probability. An efficient method for choosing values that are in Z_n^τ can turn this encryption scheme into a digital signature algorithm (if one assumes that messages that are to be signed can be represented as integers from Z_n^τ), padding the message with random bits until it becames an element from Z_n^τ is a solution, however a deterministic mechanism will be preferable.

4 Conclusion

A generalization of the discrete power function was presented which can be used as a building block for public-key cryptosystems. Also a public key cryptosystem based on this generalization is introduced. We note that this cryptosystem is not resistant against active adversaries and for this, as future work, we are interested in the use of this function in KEM/DEM frameworks in order to make the cryptosystem more efficient and to evaluate its security against active attacks such as adaptive chosen ciphertext attacks.

Acknowledgements: This work was partially supported by national research grant MEDC-CNCSIS TD-122/2007.

References:

[1] M. Abe, R. Gennaro, K. Kurosawa, Tag-KEM/DEM: A New Framework for Hybrid Encryption, *Cryptology ePrint Archive*: Report 2005/027, 2005.

[2] M. Bellare and P. Rogaway, Optimal asymmetric encryption - How to encrypt with RSA, Advances in Cryptology - Eurocrypt 94 Proceedings, *Lecture Notes in Computer Science* Vol. 950, Springer-Verlag, 1995.

[3] D. Boneh, R. Venkatesan, Breaking RSA may not be equivalent to factoring, Proceedings of Eurocrypt '98, *Lecture Notes in Computer Science*, Vol. 1233, Springer-Verlag, pp. 59-71, 1998.

[4] R. Cramer, V. Shoup, Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack, *SIAM Journal on Computing*, Volume 33 , Issue 1, pp. 167 - 226, 2004.

[5] W. Diffie, M.E. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory*, 22, 1976.

[6] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Transactions on Information Theory*, 31, 1985.

[7] K. Schmidt-Samoa, A New Rabin-type Trapdoor Permutation Equivalent to Factoring. *Electronic Notes in Theoretical Computer Science*, Volume 157, Number 3, 2006.

[8] P. Paillier, Public-Key Cryptosystems Based on Composite Degree Residuosity Classes, International Conference on the Theory and Application of Cryptographic Techniques EUROCRYPT 1999, *Lecture Notes in Computer Science*, 1592, pp. 223-238, 1999.

[9] P. Paillier, A Trapdoor Permutation Equivalent to Factoring, Second International Workshop on Practice and Theory in Public Key Cryptography, PKC '99, *Lecture Notes in Computer Science*, 1560, 1999.

[10] M. Rabin, Digitalized Signatures and Public Key Functions as Intractable as Factorization, MIT/LCS/TR-212, MIT Laboratory for Computer Science, 1979.

[11] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, 21, 1978.