Power Analysis Attacks and Countermeasures on NTRU-Based Wireless Body Area Networks

An Wang[1, 2], Xuexin Zheng[2] and Zongyue Wang[2]
[1] Institute for Advanced Study, Tsinghua University
Beijing 100084 – China
[e-mail: wanganl@tsinghua.edu.cn]
2 Key Lab of Cryptologic Technology and Information Security Ministry of Education, Shandong University
Jinan 250100 – China
*Corresponding author: An Wang

Received October 14, 2012; revised February 22, 2013; accepted March 5, 2013; published May 31, 2013

Abstract

NTRU cryptosystem has been suggested for protecting wireless body area networks, which is secure in the sense of traditional cryptanalysis. In this paper, we fulfill the first power analysis attack on the ultra-low-power environment of wireless body area networks. Specifically, two practical differential power analyses on NTRU algorithm are proposed, which can attack the existing countermeasures of NTRU. Accordingly, we suggest three countermeasures against our attacks. Meanwhile, practical experiments show that although the attacks in this paper are efficient, our countermeasures can resist them effectively.

Keywords: Cryptography, wireless body area networks, power analysis attack, NTRU

This research was supported by the National Natural Science Foundation of China (Grant No. 61133013 and 60931160442) and the Tsinghua University Initiative Scientific Research Program (No.2009THZ01002, No.20111080970). Besides, we are grateful to the reviewers and the editor that contributed to the great improvement of the original version of this paper with their valuable comments and suggestions.

http://dx.doi.org/10.3837/tiis.2013.05.009

1. Introduction

Nowadays, wireless body area networks (WBAN) [1] have been widely applied in people's daily life. They usually consist of intelligent and small devices implanted in or attached on the body which can establish a wireless communication channel. The devices provide continuous health monitoring and real-time feedback to their owner or medical personnel. What's more, the devices can record measurements for a long time, improving the quality of the measured data. WBAN node usually comprises a biosensor or a medical device with sensing unit for some medical purposes.

In practice, it's very important to guarantee the security of sensitive data in WBAN. So, schemes of encrypted communication and authentication should be design, and some cryptographic algorithms [2] are employed for implementing them. However, in WBAN, the designers face serious restriction on the amount of computational power, gate area, and memory storage that are allowed to be consumed by tiny sensors [3]. Hu et al. suggested that NTRU cryptosystem [4, 5, 6] can be adopted for encryption communication and authentication due to its high efficiency [7, 8]. In the sense of traditional cryptanalysis, NTRU cryptosystem can solve the security problem of WBAN.

However, in 1999, Kocher et al. proposed differential power analysis (DPA) attack [9] which recovered the secret key by analyzing the instantaneous power consumption of a running chip. This kind of attacks is much more effective than traditional cryptanalysis. Although some masking schemes [10, 11] have been designed against DPA, there are still successful attacks [12, 13] on these countermeasures in the past few years. For NTRU cryptosystem, Lee et al. gave some attacks and three countermeasures, and asserted that their countermeasures can resist second-order DPA [14].

In this paper, we make the following contributions on NTRU-based WBAN.

- The experiment environment of power analysis attacks on WBAN is built, and the feasibility of DPA in an ultra-low-power environment is verified based on two experiments.
- We point out the flaw of existing countermeasures that the output of convolution product may bring some leakages. According to the comparison between differential traces corresponding to output of convolution product, two new DPAs on NTRU are proposed. Our experiments show that they can break the existing countermeasures efficiently.
- Three countermeasures against our attacks are suggested, which can resist the existing attacks effectively according to our experiments.

This article is organized as follows. In Section 2, we review the security of WBAN, NTRU cryptosystem, and its countermeasures against DPA. Then, Section 3 shows the principle and our setups of DPA. In Section 4, we propose new attacks on non-protected and protected NTRU respectively. In Section 5, we suggest some countermeasures against our attacks. Finally, we conclude this article in Section 6.

2. Preliminaries

2.1 Related Works: Security of WBAN

In WBAN, the transfer of health information between sensors and servers over the wireless channel and Internet should be private and confidential [15] because the adversary may tamper the health data, submit shoddy data, get user's privacy, etc. Accordingly, some authentication and encryption protocols should be designed for WBAN security. Due to the restricted resources, some light weight cryptographic schemes are employed [16, 17].

As IEEE 1363.1 standard [5], NTRU public key cryptosystem [4] which is a typical light weight scheme has been proposed for encryption communication of wireless sensor network [18]. Hu et al. gave implementation of NTRU based on low-power hardware [8]. Then, Hu et al. suggested NTRU system protecting implantable medical device [19] because its simplification can greatly save local CPU energy consumption.

Non-protected NTRU system cannot resist the power analysis attack. In 2008, Atici et al. gave the first power analysis on NTRU [20]. Then, Lee et al. proposed DPA and second-order DPA on NTRU, gave three countermeasures against DPA, and asserted that their countermeasures can resist second-order DPA [14]. Section 2.3 introduces the details of their countermeasures.

Under the environment of WBAN, power analysis can be mounted in a way that is described in **Fig. 1**. First, the adversary acquires the power consumption with a differential probe and oscilloscope. Then, the NTRU private key is recovered. So, an identification of legal user or administrator can be forged, which can be used for gaining the information by cheating. Although this information may be ciphertext, it can still be decrypted by the NTRU key.

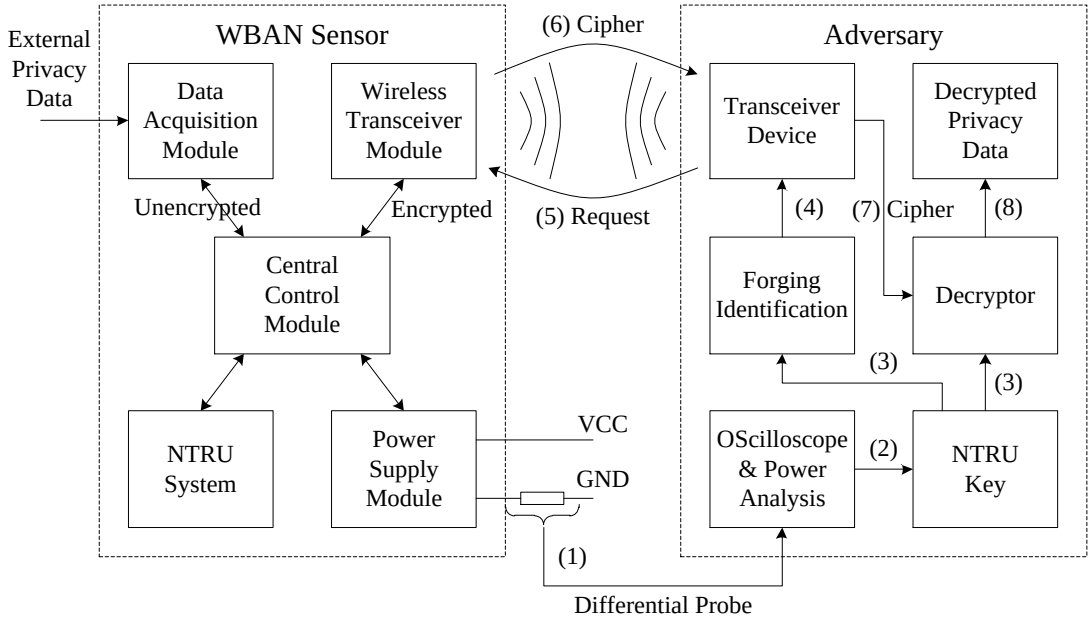

Fig. 1. Power attack process on NTRU-based WBAN Sensor

2.2 NTRU Cryptosystem

NTRU cryptosystem [4, 5] is based on the algebraic structures of polynomial ring

$$R = Z[x]/(x^N - 1).$$

An element $f \in R$ will be written as a polynomial or a vector

$$f = \sum_{i=0}^{N-1} f_i x^i = [f_0, f_1, ..., f_{N-1}].$$

The multiplication in *R* is given explicitly as a cyclic convolution product, $f * g = h$ with

$$h_k = \sum_{i=0}^{k} f_i g_{k-i} + \sum_{i=k+1}^{N-1} f_i g_{N+k-i} = \sum_{i+j \equiv k \bmod N} f_i g_j .$$

f modulo *q* means reducing the coefficients modulus *q*, and the inverse of *f* mod *q* is defined as the polynomial f^{-1} satisfying

$$f * f^{-1} \equiv 1 \bmod q$$

in the polynomial ring *R*.

The integer *N* decides the ring *R*, and *p* and *q* are respectively small and large modulus. The private key $f = 1 + pF$ is invertible modulo *q*, where *F* is a binary polynomial with *d* nonzero coefficients. The public key

$$h = f^{-1} g \bmod q$$

is known to everyone, while *g* is a small polynomial kept secret by the owner. For the encryption, let *m* be the polynomial representing a message. We choose a small polynomial *r* as the random blinding polynomial, and compute the ciphertext

$$c = p * r * h + m \bmod q .$$

For the decryption of *c*,

$$a = f * c \bmod q$$

is computed firstly, where the modulus *q* operation is done in an appropriate interval. Then the plaintext

$$m = a \bmod p$$

is recovered.

As we can see, the dominant operation in the encryption and decryption of NTRU is the multiplication of two polynomials in the ring *R*. We take decryption for example to explain convolution product and DPA. During the decryption, it is common practice to compute

$$f * c \bmod q = c + p * F * c \bmod q .$$

The recovery of *F* means a successful attack, so we focus on the computation $F * c \bmod q$. Notice that *F* is a binary polynomial with fixed nonzero coefficients, and *c* has coefficients that are distributed almost randomly. **Fig. 2** shows the computation of

$$t = F * c \bmod q .$$

Here *c* is denoted as *N* coefficients $[c_0, c_1, ..., c_{N-1}]$, and the binary polynomial *F* is represented as an array *b* which indicates the *d* nonzero locations. For example,

$$F(x) = x + x^4 + x^5 + x^7 = [0,1,0,0,1,1,0,1]$$

for $N = 8$ will be represented simply as $b = [1,4,5,7]$.

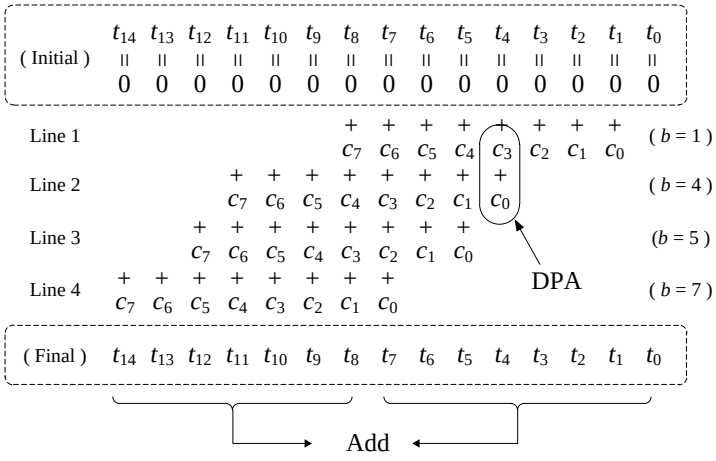

Fig. 2. Computation of convolution product $t = F * c \bmod q$ of NTRU

2.3 DPA and Countermeasures on NTRU

Lee et al. gave DPA on NTRU [14] based on Hamming distance model which assumed that the power consumption has positive linear relationship to the Hamming distance of two intermediate values [21]. As is described in **Fig. 2**, when c_0 is added to t_4 (Now $t_4 = c_3$) in line 2, the instantaneous power consumption will leak the Hamming distance between c_3 and c_3+c_0. So, $b[1]-b[0]$ can be recovered. After all the $b[i]-b[i-1]$ $(i=1,2,...,N-1)$ are gotten, an exhaustive search of $b[0]$ can recover the whole secret key.

In order to blind the intermediate information during convolution product, Lee et al. gave the following countermeasures [14].

- Random initialization of t. Every register t_i $(i=0,1,...,2N-2)$ is added by a random number r_i at the beginning of convolution computation. After the convolution is done, these r_i are subtracted from the corresponding register t_i.
- Blinding c using random values. For the original input values c_i $(i=0,1,...,N-1)$, the countermeasure is to replace them by $c_i + r$, where r is a random integer. For a correct decryption, the output of convolution product is replaced by $t_j + t_{j+N} - dr \bmod q$.
- The third countermeasure is randomization of b. The randomized order of $b[i]$ disables the statistical analysis of $b[i]-b[i-1]$ in their attack.

However, we think that blinding in convolution product is not enough, and the output of convolution product may bring some leakages because the information of real t will be exposed by DPA finally. Specially, some plaintexts can be carefully chosen for an attack. Although output is forbidden when an illegal intermediate value is detected, DPA can still get this information. We show these attacks in Section 4.

3. Setup of DPA on WBAN

We first built a simulation environment of WBAN in order to mount a DPA attack, which is described in **Fig. 3**. The ultra-low-power microprocessor ATmega168 was employed for executing an NTRU algorithm. We implemented the convolution product with the parameters $N = 63$ and $d = 17$. For reducing the noises, a DC stabilized power supply Agilent E3616A was adopted. We connected a resistor of 10 ohm between the power supply and microprocessor, and used a differential probe and oscilloscope Agilent DSO90404A for acquisition of instantaneous voltage which was related to the power consumption of microprocessor. Meanwhile, a high impedance adapter Agilent E2697A including 500MHz passive probe was used for getting trigger signals and location of interesting samples.

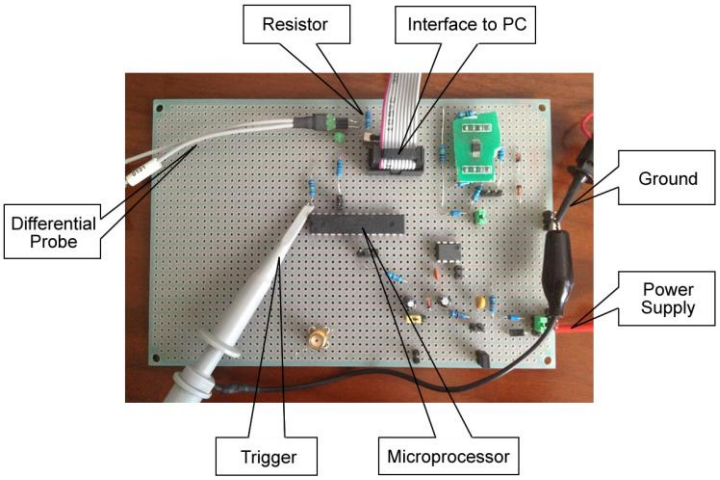

Fig. 3. Experiment board of power analysis attacks

We made two experiments to verify the effect of power analysis. First, let microprocessor execute an LDI instruction for loading immediate value. We loaded 00, 01, 03, 07, 0F, 1F, 3F, 7F, FF (in hexadecimal format) respectively. For each value, we executed 1 000 LDI instruction, so 1 000 traces and their average trace could be acquired. The nine average traces are shown in **Fig. 4**, which follows the Hamming weight model [22].

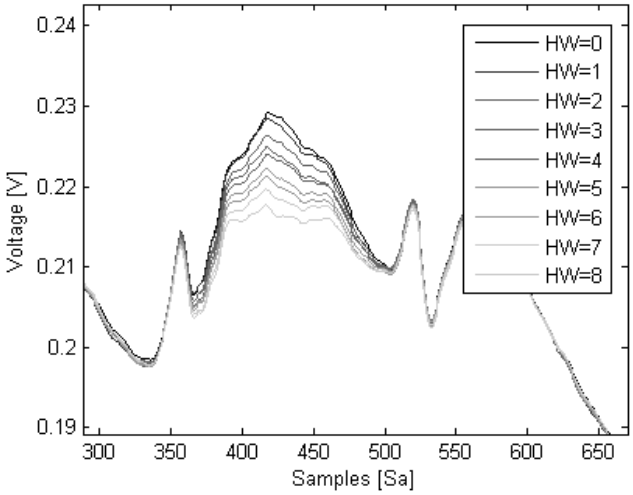

Fig. 4. Average power traces of LDI instructions with nine values

Our second experiment showed DPA attack of Lee et al. [14]. We changed n different ciphertexts and decrypted them for n times, and then n traces would be got. We focused on the moment when c_0 was added to some t_i in line 2 (Refer to **Fig. 2** and assumed t_i is from c_w to c_w+c_0 now). For each guess w, we could compute the correlation coefficient between the n traces and the n Hamming distances of (c_w, c_w+c_0). So, the w corresponding to the greatest correlation coefficient was equal to $b[1]-b[0]$. **Fig. 5** shows the result of this attack, and the correct guess of $w=3$ corresponding to the only black line was recovered.

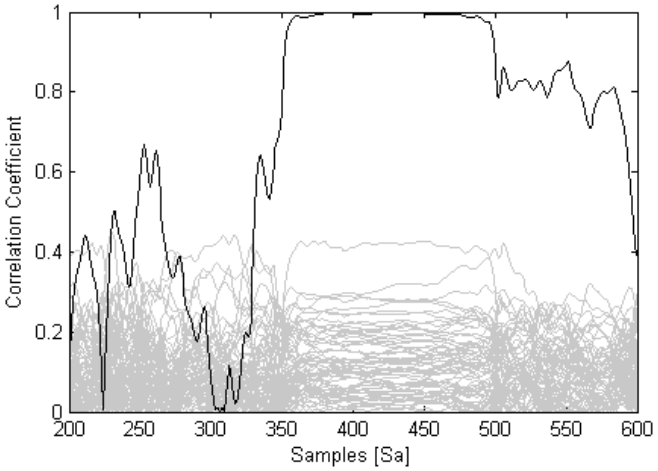

Fig. 5. Correlation power anlaysis on non-protected NTRU

4. Differential Power Analysis on NTRU

The attack above can break non-protected NTRU. However, three countermeasures from Lee et al. can resist on this kind of first-order DPA attack. In this section, we propose new DPA attacks on the three countermeasures of NTRU. Our attacks are chosen-ciphertexts attack, which can be mounted on a system whose input is not restricted (called non-protected NTRU here). However, some NTRU systems can detect the validity of input (called protected NTRU). So, two cases are discussed respectively.

4.1 DPA on Non-Protected NTRU

To attack an NTRU decryption system, an adversary can choose two ciphertexts and make two experiments. Assume that the ciphertext c is denoted as $[c_0,c_1,...,c_{N-1}]$. First, choose $[0,0,0,...,0]$ as ciphertext and make 100 decryptions. An average trace is acquired, denoted by T_1. Then, choose $[a,0,0,...,0]$ as ciphertext and make a same experiment, T_2 can be got. Here a should be a valid coefficient which has the maximum Hamming weight so that the power consumption of operating a shows more significant difference from that of zero. So, $\Delta T=|T_1-T_2|$ which includes some peaks (deriving from the above difference) can be figured out. We focus on the part of ΔT corresponding to the operation of $[t_0,t_1,...,t_{N-1}]+[t_N,t_1,...,t_{2N-2}]$. The position of a in $[t_0,t_1...,t_{2N-2}]$ can be recovered according to the position of peaks in ΔT. Therefore, the secret key can be recovered directly. Fig. 6 shows the principle of this attack, which take $b=[1,4,5,7]$ for example.

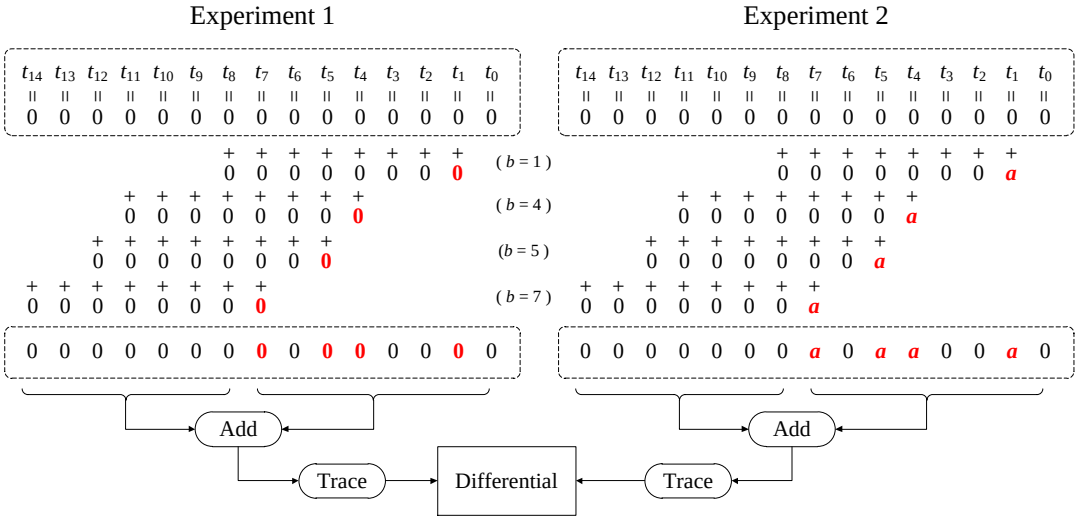

Fig. 6. Differential power anlaysis on non-protected NTRU

Remark. Usually, NTRU cryptosystem can detect illegal intermediate results such as the result of convolution product, and stop the decryption. So, some chosen-ciphertext attack is infeasible in the sense of traditional cryptanalysis. However, DPA can still get this intermediate information by the "side-channel" although the output is forbidden.

4.2 DPA on Protected NTRU

If NTRU system can detect the invalidity of input, we give a general method in this section. The process of attack is the same with Section 4.1. The only difference is that the two ciphertexts are chosen as $[a,c_1,c_2,...,c_{N-1}]$ and $[b,c_1,c_2,...,c_{N-1}]$ respectively. Here, all the $c_i(i=1,2,...,N-1)$ are valid coefficients, while a and b are two valid coefficients and the difference of their Hamming weights is as large as possible. Similarly, the position which a has added to can be recovered according to the position of peaks in ΔT, and the secret key can be recovered. **Fig. 7** shows the principle of this attack.

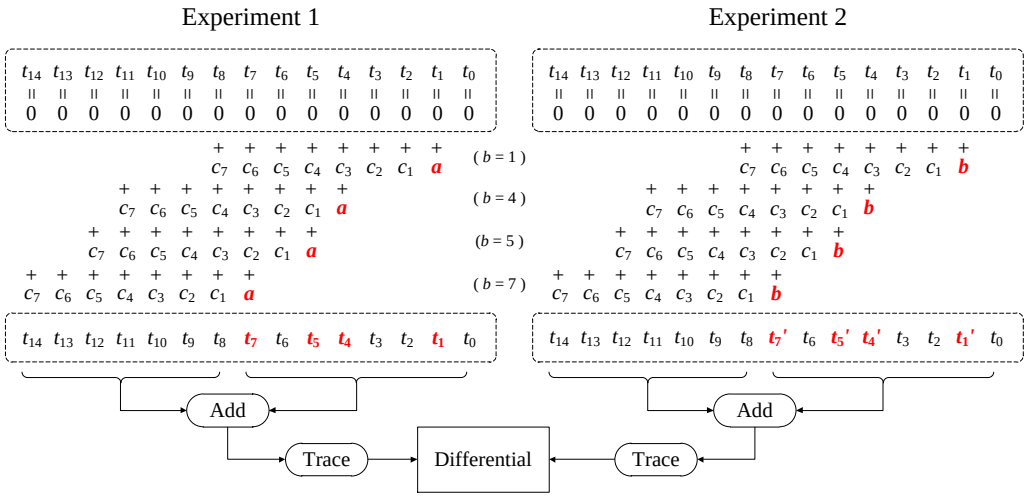

Fig. 7. Differential power anlaysis on protected NTRU

Remark. Some key bits may not be recovered in this attack with a very low probability because of the coincidence when the Hamming weight $\mathrm{HW}(t_i) = \mathrm{HW}(t_i')$. Choosing another ciphertext and repeating this attack once more will solve this problem.

4.3 Experiments and Efficiency

We implemented NTRU decryption with $N = 63$ and $d = 17$, and the secret key was set to b = [1, 4, 5, 7, 12, 15, 19, 24, 28, 33, 36, 39, 42, 47, 51, 55, 60]. The attack of Section 4.1 was mounted, and two traces were acquired, both of which were averaged from 100 original traces. **Fig. 8** shows the two average trace (top and middle) and their differential trace (bottom), in which every 4 000 sampling points correspond to a t_i, and 63 t_i in all (traces corresponding to $t_{64}, t_{65}, ..., t_{125}$ are omitted because of independence of secret key). Obviously, the secret key was recovered correctly.

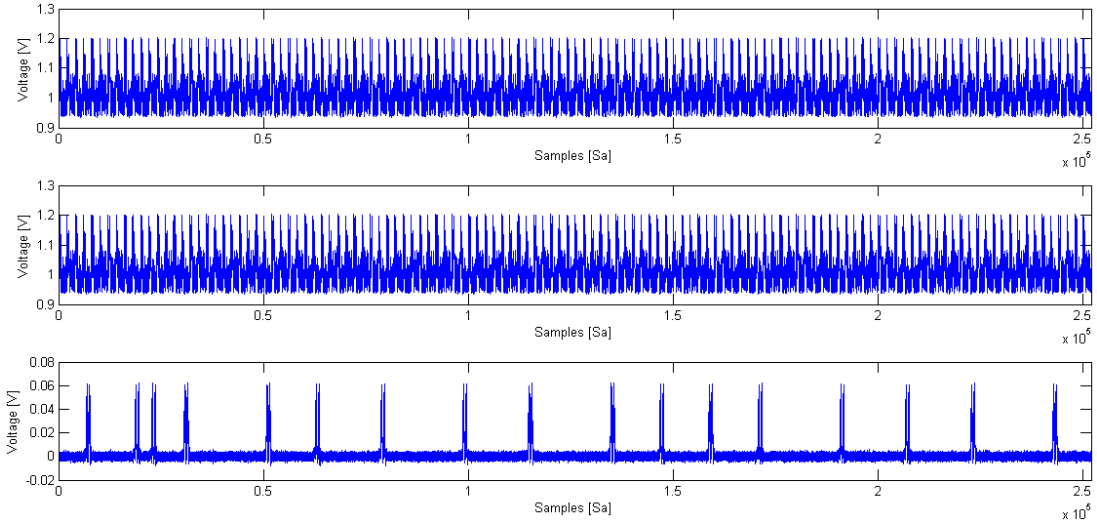

Fig. 8. Differential power anlaysis on non-protected NTRU

Subsequently, we made an experiment of DPA on protected NTRU, which is described in **Fig. 9**. Although the signal to noise ratio was a little less, the secret key was recovered correctly.

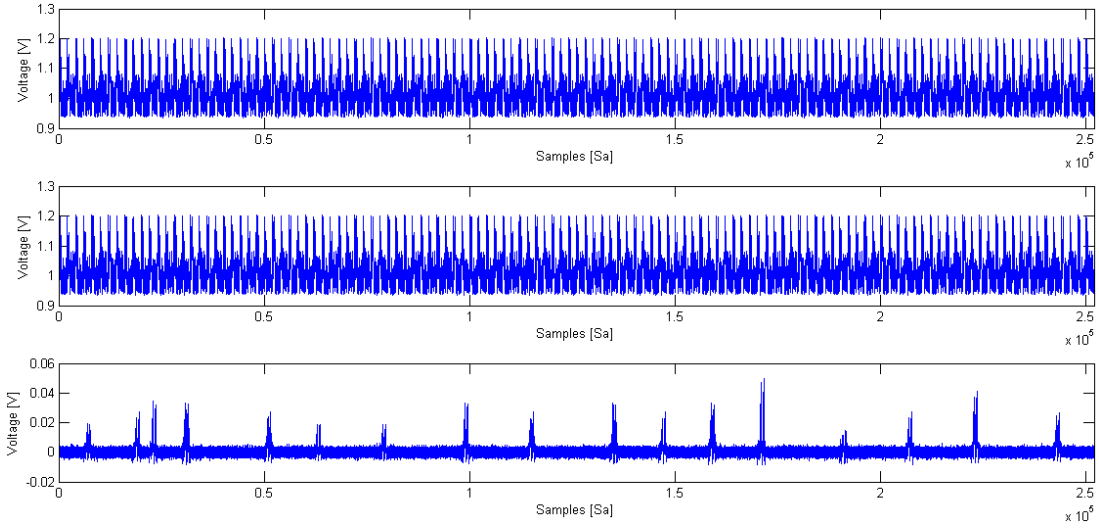

Fig. 9. Differential power anlaysis on protected NTRU

Table 1 shows the comparison between DPAs in this paper and correlation power analysis (CPA) of Lee et al. [14]. During our DPAs, only 200 traces are needed, but CPAs need much more. For a sampling point, only one subtraction is computed in our DPAs, and a correlation coefficient is computed at least in CPAs. The three countermeasures proposed by Lee et al. can resist on their CPA, and limit the effect of 2-order CPA, but our DPAs can break them. What's more, after the computation of correlation coefficient, their CPAs need an extra exhaustive search, but our DPAs can recover the secret key directly.

Table 1. Comparison between our attacks and some existing ones

Attacks	Num. of traces	Computation complexity	Attack on countermeasures	Subsequent search
CPA [14]	1 000	ρ	Cannot break	Need
2-Order CPA [14]	10 000	$\rho + s$	Limited	Need
Our DPA (4.1)	200	s	Can break	Needn't
Our DPA (4.2)	200	s	Can break	Needn't

5. Countermeasures

The attacks presented in this paper defeat three existing countermeasures of NTRU. However, we think there are some countermeasures against our attacks, which is appropriate for the WBAN environment.

– Random delays. In the "differential" idea, the most important condition is horizontal alignment between the two traces. So, we can tries to complicate data alignment against DPA. These misregistrations of traces reduce the SNR significantly, so that cryptographic devices can be well protected. Some random delays are inserted into the cryptographic operation either by special state machines or non-deterministic processors [23]. In software implementation, some null operations such as NOP can be inserted, whose number can be randomly chosen. What's more, in hardware

implementation, some random delay elements consisting of buffers can be connected in series, which can randomize the execution time of arithmetic module.

– Masking. Before the computation of convolution product, randomly choose masks r_i $(i = 0,1,2,...,2N-2)$ and add them to t_i. After convolution product, r_i is not removed momentarily. Instead, we compute

$$m_i = [(t_i + r_i) \bmod p - r_i \bmod p] \bmod p$$

for getting the coefficients of message. So, when the mask is removed at last, each coefficient only has about $\log p$ bits information, which is much less than the $\log q$ bits information of the old countermeasures because $p << q$.

– Dummy operations. NTRU decryption includes one convolution product and one modular arithmetic, but it can also be implemented with some other dummy convolution products and modular arithmetic. These dummy operations run the same operations with standard NTRU, but their results don't join the standard computation. As a result, the attacker will get some invalid information with high probability due to the confusion of the dummy operations.

We implemented the above countermeasures in software. Specifically, besides the help of masks, $0-31$ NOP instructions were randomly chosen and inserted into the beginning of sensitive operations. Three dummy convolution products and modular arithmetic joined the program. We tried to mount the DPA attack of Section 4.2 on these countermeasures, which is showed in **Fig. 10**.

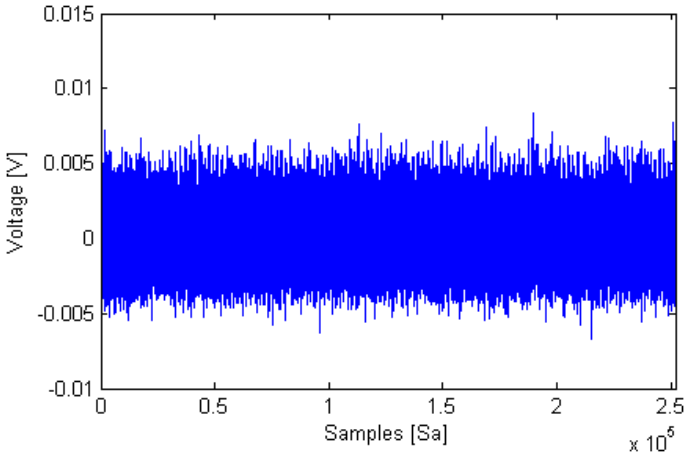

Fig. 10. Differential power anlaysis on our countermeasures

In fact, the masking countermeasure decreases the frequency of the original peaks so that much less information is leaked. The random delays countermeasure spreads each peak to both sides, so it can make the peaks lower. What's more, the dummy operation can also linearly lower the peaks. Obviously, it is hard to get information from the implementation of our countermeasures.

6. Conclusions

In this paper, we give two power analysis attacks on NTRU-based WBAN and three countermeasures against our attacks. Our attack is effective because of the lack of external blinding for convolution product. In the future, we will try to find a complete blinding and padding scheme of NTRU which covers the whole process of decryption.

We think that there are some other attacks whose efficiency is higher than our differential power analysis attacks. In the field of side-channel attack, the wireless channel also encounters some other attack, such as differential electromagnetic analysis, carrier wave based power analysis, etc. So, we will try to combine these attacks for getting more information in the future.

References

[1] B. Latre, B. Braem, I. Moerman, C. Blondia, P. Demeester, "A survey on wireless body area networks," in *Proc. of Wireless Networks*, vol. 17, no. 1, pp. 1-18, Springer, Heidelberg, 2011.
Article (CrossRef Link)

[2] A.J. Menezes, P.C. Van Oorschot, and S.A. Vanstone, *Handbook of applied cryptography*. CRC Press, 1997.
Article (CrossRef Link)

[3] A. Perrig, R. Szewczyk, JD. Tygar, V. Wen, DE. Culler, "Spins: security protocols for sensor networks," in *Proc. of Wireless Networks*, vol. 8, no. 5, pp. 521-534, Springer, Heidelberg, 2002.
Article (CrossRef Link)

[4] J. Hoffstein, J. Pipher, J. Silverman, "NTRU: A ring-based public key cryptosystem," in *Proc. of Algorithmic Number Theory (ANTS III)*. LNCS, vol. 1423, pp. 267-288, Springer, Heidelberg, 1998.
Article (CrossRef Link)

[5] IEEE Std P1363.1-2008, "IEEE standard specification for public key cryptographic techniques based on hard problems over lattices," 2009.
Article (CrossRef Link)

[6] J. Hoffstein, J. Pipher, J.H. Silverman, "NSS: An NTRU lattice-based signature scheme," in *Proc. of Eurocrypt 2001*, LNCS, vol. 2045, pp. 211-228, Springer, Heidelberg, 2001.
Article (CrossRef Link)

[7] F. Hu, Q. Hao, M. Lukowiak, Q. Sun, K. Wilhelm, S. Radziszowski, Y. Wu, "Trustworthy data collection from implantable medical devices via high-speed security implementation based on IEEE 1363," *IEEE Transactions on Information Technology in Biomedicine*, vol. 14, no. 6, pp. 1397-1404, 2010.
Article (CrossRef Link)

[8] F. Hu, K. Wilhelm, M. Schab, M. Lukowiak, S. Radziszowski, Y. Xiao, "NTRU-based sensor network security: a low-power hardware implementation perspective," *Security Comm. Networks*. vol. 2009, no. 2, pp. 71-81, 2009.
Article (CrossRef Link)

[9] P. Kocher, J. Jaffe, B. Jun, "Differential power analysis," in *Proc. of Crypto 1999*, LNCS, vol. 1666, pp. 388-397, Springer, Heidelberg, 1999.
Article (CrossRef Link)

[10] D. Canright, L. Batina, "A very compact perfectly masked S-Box for AES," in *Proc. of ACNS 2008*, LNCS, vol. 5037, pp. 446-459, Springer, Heidelberg, 2008.
Article (CrossRef Link)

[11] H. Kim, S. Hong, J. Lim, "A fast and provably secure higher-order masking of AES S-Box," in *Proc. of CHES 2011*, LNCS, vol. 6917, pp. 95-107, Springer, Heidelberg, 2011.
Article (CrossRef Link)

[12] C. Clavier, B. Feix, G. Gagnerot, M. Roussellet, V. Verneuil, "Improved collision-correlation

power analysis on first order protected AES," in *Proc. of CHES 2011*, LNCS, vol. 6917, pp. 49-62, Springer, Heidelberg, 2011.
Article (CrossRef Link)

[13] A. Moradi, O. Mischke, T. Eisenbarth, "Correlation-enhanced power analysis collision attack," in *Proc. of CHES 2010*, LNCS, vol. 6225, pp. 125-139, Springer, Heidelberg, 2010.
Article (CrossRef Link)

[14] M. Lee, J. Song, D. Choi, D. Han, "Countermeasures against the power analysis attack for the NTRU public key cryptosystem," *IEICE TRANSACTIONS on Fundamentals of Electronics*, vol. E93-A, no. 1, pp. 153-163, 2010.
Article (CrossRef Link)

[15] A. Bhargava, M. Zoltowski, "Sensors and wireless communication for medical care," in *Proc. of 14th International Workshop on Database and Expert Systems Applications*, pp. 956-960, 2003.
Article (CrossRef Link)

[16] G. Selimis, L. Huang, F. Masse, I. Tsekoura, M. Ashouei, F. Catthoor, J. Huisken, J. Stuyt, G. Dolmans, J. Penders, H. Groot, "A lightweight security scheme for wireless body area networks: design, energy, evaluation and proposed microprocessor design," *Journal of Medical Systems*, vol. 2011, no. 35, pp. 1289-1298, 2011.
Article (CrossRef Link)

[17] M. Mana, M. Feham, B. Bensaber, "A light weight protocol to provide location privacy in wireless body area networks," *International Journal of Network Security & Its Applications*, vol. 3, no. 2, pp. 1-11, 2011.
Article (CrossRef Link)

[18] P. Xiong, W. Zhang, G. Lu, "Secure neighbor relation in wireless sensor network," in *Proc. of 4th International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1-4, IEEE, 2008.
Article (CrossRef Link)

[19] F. Hu, Q. Hao, M. Lukowiak, "Implantable medical device communication security: pattern vs. signal encryption (position paper)," in *Proc. of the 2nd USENIX Conference on Health Security and Privacy*, pp. 1-2, USENIX Association, 2011.

[20] A. Atici, L. Batina, B. Gierlichs, I. Verbauwhede, "Power analysis on NTRU implementations for RFIDs: First results," in *Proc. of RFIDSec 2008*, pp. 128-139, 2008.

[21] E. Brier, C. Clavier, F. Olivier, "Correlation power analysis with a leakage model," in *Proc. of CHES 2004*, LNCS, vol. 3156, pp. 16-29, Springer, Heidelberg, 2004.
Article (CrossRef Link)

[22] S. Mangard, E. Oswald, T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*, Springer, Heidelberg, 2007.
Article (CrossRef Link)

[23] J. Irwin, D. Page, N.P. Smart, "Instruction stream mutation for non-deterministic processors," in *Proc. of IEEE International Conference on Application-Specific Systems, Architectures and Processors*, pp. 286-295, IEEE Computer Society, Los Alamitos, 2002.
Article (CrossRef Link)

An Wang was born in 1983. He received his PH.D. degree in Shangdong University in 2011. He currently works as a postdoctor in Tsinghua University. His main research interests include side-channel attack, embedded system, and fast implementation in cryptography. He is also the webmaster of a cryptographic website (http://www.mathmagic.cn).

Xuexin Zheng was born in 1987. She received his B.S. degree in Shangdong University in 2008. She is currently a Ph.D. student in the Key Lab of Cryptographic Technology and Information Security Ministry of Education, Shandong University. Her main research interests include lattice-based cryptography, power analysis attack, and cryptanalysis.

Zongyue Wang was born in 1988. He received his B.S. degree in Shangdong University in 2010. He is currently a Ph.D. student in the Key Lab of Cryptographic Technology and Information Security Ministry of Education, Shandong University. His main research interests include embedded system and system on chip (SoC).