Call for Proposals

Network & Information security Technology

HIRP OPEN 2017

Application Deadline: 09:00 A.M., 16th June, 2017 (Beijing Standard Time, GMT+8).

If you have any questions or suggestions about HIRP OPEN 2017, please send Email (innovation@huawei.com). We will reply as soon as possible.

Catalog

HIRPO2017120301: Low latency and low cost consensus algorithm for blockchain

1 Theme: Network & Information security Technology

2 Subject: Blockchain Consensus Optimization

List of Abbreviations

PBFT: Practical Byzantine Fault Tolerance;

PoET: Proof of Elapsed Time;

PoS: Proof of Stake;

PoW: Proof of Work;

IoT: Internet of Things;

SGX: Software Guard eXtensions;

TEE: Trusted Execution Environment.

3 Background

The consensus protocols for public and permissionless blockchains usually require long time of delay before transaction confirmation. For Bitcoin, it averagely takes 10 minutes to create a block while about an hour till its final confirmation. For Ethereum, it takes about 15 seconds to form a block. If we consider IoT devices-based payment system, a delay of 15 seconds is still unacceptable. Considering Hyperledger Fabric (which uses PBFT as the default consensus algorithm), the confirmation delay can be reduced to less than 1 second, which seems to be acceptable when used in a payment system relying on IoT devices. However, when the number of validating peers (nodes that record full block data and validate transactions, like miners in Bitcoin

system) is more than 20, the performance of PBFT deteriorates significantly. Accordingly, the optimization of consensus delay for delay-sensitive blockchain applications, where the distributed nodes are massively deployed, is a critical problem to be mitigated.

4 Scope

We expect a significant performance escalation using improved consensus algorithm together with other novel blockchain technologies. The preliminary application is the IoT device-based payment system, where the power and computation capabilities are typically constrained. There currently seems no suitable solution to satisfy the following requirements (be subject to change during the development):

1. Short confirmation time of transactions (less than 1 second) when there are more than 100 validating peers.
2. Cost efficient (less than $0.01 per transaction).

There are wide researches in public blockchain, such as Proof of Stake (PoS), which can make the cost per transaction low compared to the preceding PoS. Hardware-secure device based consensus has recently become an attractive trend, which bases on the hardware-secure TEE, such as Intel's SGX and ARM's TrustZone, for optimizing the consensus in terms of algorithm complexity and confirmation speed. Intel has recently contributed the "Sawtooth Lake" to Hyperledger open project, which depends on the SGX to achieve consensus by introducing a new algorithm PoET, which mainly target to the consortium blockchain. For achieving the goals above, new technologies can be developed, or rely on the framework of some existing blockchain prototypes.

We expect a related paper to be published in the following conferences or journals:

- Conferences: Level 1: Crypto, Eurocrypt, Asiacrypt, CCS, S&P, NDSS, USENIX, ESORICS, PKC
- Level 2: CT-RSA, FC, AsiaCCS, ACNS, SecureComm, TrustComm
- Journals: Journal of Cryptology, TDSC, TIFS, TISSEC, JCS, DCC, IJIS

5 Expected Outcome and Deliverables

- The invention of the low-latency and low-cost consensus algorithm with one related patent idea and one research paper are expected.
- A technical report on existing blockchain technologies is expected.
- A final prototype for performance evaluation.

6 Acceptance Criteria

- Two main performance requirements are considered:
  - The consensus time for each transaction is less than 1 second, given validating node number over 100.
  - The overall cost for each confirmed transaction is less than $0.01.
- The patents should be reviewed by the technical committee by Huawei.
- The research papers should be published in the list of suggested conferences and journals listed above.
- The technical report should be reviewed by the technical committee by Huawei.

7 Phased Project Plan

The term of this project lasts for 1 year (divided by 4 phases, and 3 months for each).

Phases: 1: Survey the existing blockchain technologies, conduct deep research and finalize the techniques that will be used. Specially consider the hardware secure devices, for serving the consensus.

Phase: 2-3: Conduct the development, complete milestone reporting and performance evaluation. Deliver the patent idea related to the consensus algorithm.

Phase 4: Test and finalize the work by delivering the prototype. Productize the inventions depending on the possibility. One publication in the suggested prominent conferences or Journals is expected.

Click here to back to the Top Page

HIRPO2017120302: Practical NTRU with provable security

1 Theme: Network & Information security Technology

2 Subject: Post Quantum Cryptography, Lattice-based Cryptography

3 List of Abbreviations

raw NTRU/original NTRU: The NTRU encryption scheme devised by Hoffstein, Pipher and Silverman

4 Background

Current public-key cryptographic algorithms in use nowadays will be considerably impacted by the arrival of large-scale quantum computers. With Shor's algorithm, today's public-key algorithms will become insecure, including RSA, Elliptic-Curve Cryptography (ECC), Diffie-Hellman and pairing-based cryptography.

NTRU is considered as the most viable post-quantum public key encryption [PC09]. Nowadays, NTRU is commonly considered as a reasonable alternative to the encryption schemes based on integer factorization and discrete logarithm over finite fields and elliptic curves, as testified by its inclusion in the IEEE P1363 standard [IEEE1363].

In terms of security and efficiency, the raw NTRU is defined over a polynomial ring $R = \mathbb{Z}[x] / (x^n - 1)$ with $n = 257$. The secret key consists of two

sparse polynomials (f,g) of degrees $<n$ and coefficients in $\{-1,0,1\}$. The public key $h=f/g \bmod q \in R_q^*$ is their quotient in the ring $R_q = \mathbb{Z}_q[x]/(x^n-1)$ (the denominator is resampled if it is not invertible). The underlying intuition is that public key h looks like a uniformly distributed of R_q. As [SS11] pointed out, the raw NTRU is not secure in the sense of IND-CPA.

Motivated by the uncertainty over the security of NTRU, [SS11] and [SS13] achieve IND-CPA security from the hardness of R-SIS and R-LWE over ideal lattice. They defined the NTRU variant over the polynomial ring $R=\mathbb{Z}[x]/(x^n+1)$. The private key (f,g) are sampled from the discrete Gaussian distribution D_σ^* to ensure that the distribution of $h=f/g$ is statistically close to uniform over R_q^*. Based on the requirement of smoothing parameter of the underlying lattices, they finally determined the deviation parameter $\sigma \approx n^c q^{\frac{1}{2}} > q^{\frac{1}{2}}$. The NTRU variant proposed in [SS11] and [SS13] are constructed via the tools such as discrete Gaussian sampling, smoothing parameter, Fourier analysis. Since all of these tools have found common use today in the field of lattice-based cryptography, Stehlé and Steinfeld are possibly in the right direction to tailor raw NTRU into a provably secure one. However, the practical instantiations are likely to be significantly less efficient than the original schemes, as stated by the authors.

5 Scope

This research collaboration considers both academic breakthrough and industrial application. In other words, we hope that the new NTRU variant can achieve provable security while maintaining efficiency, and it is expected to

outperform those existing schemes ([SS11] and [HS03]) in terms of security and efficiency.

5.1 Constructing Novel Provable Secure NTRU Scheme

The aim for this part is to construct novel provably secure NTRU scheme, which is applicable to resource constrained computing device such as individual subscribers and home network nodes.

As a result, the following three requirements should be met at the same time:

- **Security**: A solid theoretical ground for the security of the proposed NTRU scheme should be given in the asymptotic sense, and have much better assurance of quantum safety.
- **Efficiency:** There are two aspects in this requirement, namely:
  - Less computation time related to Key Generation, Encryption and Decryption.
  - Smaller key size, low ciphertext expansion, etc.
- **Application**: The above provably secure NTRU variant is expected to be used in a lightweight manner, i.e., it is suitable for using in individual subscribers, home network nodes and some other resource constrained devices in IoT scenario.

The foreseeable tasks include (but not limited to): new algebraic structure (ring, etc) to define NTRU; algorithms construction; security proof.

Since new algebraic ring will be explored to define novel NTRU, the existing tools such as discrete Gaussian sampling, smoothing parameter, Fourier analysis and so on may not be directly applied. Therefore there is potential requirement of tailoring such tools for the new algebraic structure and determining the specific application form like [SS11] and [SS13].

Comparison with existing schemes such as [SS11] is highly preferred. The

expected throughput loss (compared to raw NTRU) is less than 30%. The security model and assumptions must be clearly stated.

The related paper should be published in the following conferences or journals:

- Conferences: Level 1: Crypto, Eurocrypt, Asiacrypt, CCS, S&P, NDSS, USENIX, ESORICS, PKC
- Level 2: CT-RSA, FC, AsiaCCS, ACNS, SecureComm, TrustComm
- Journals: Journal of Cryptology, TDSC, TIFS, TISSEC, JCS, DCC, IJIS

5.2 Prototype of the novel NTRU

The aim for this part is to implement the prototype and check whether it complies with original design.

The foreseeable tasks include (but not limited to): implementing the scheme; determining four groups of scheme parameters corresponding to 56-bit, 80-bit, 128-bit and 256-bit security; developing the elementary arithmetic patent for accelerated computing, which is similar to the discrete Fourier transform for multiplying polynomials.

6 Expected Outcome and Deliverables

- A technical report is expected to summarize the algebraic tools involved in this research.
- Two patents and one research papers are expected.
- A prototype and a design report are expected for provably secure NTRU on 56-bit security construction.

7 Acceptance Criteria

- Prototype on 56-bit security construction: It should occupy RAM<5KB,

ROM<50KB.

- The patents should be reviewed by the technical committee by Huawei.
- The research papers should be published in the list of suggested conferences and journals listed above.
- The technical report should be reviewed by the technical committee by Huawei.

8 Phased Project Plan

Duration: 1.5 year, 6 phases with 3 months each.

- Phase 1-2: Research for exploring and determining the algebraic structure to be used. A technical report is expected to cover:
- The existing algebraic tools used in lattice such as discrete Gaussian sampling (the ins and outs of smoothing parameter over lattice, Poisson summation over duality lattice, etc), Fourier analysis and so on.
- The detailed description of the new algebraic structure as well as its key algebraic properties in both algebraic and geometrical manner.
- Phase 3-4: Research and design practical NTRU with provable security. It should have less than 30% throughput loss when compared with raw NTRU. A patent related to fast implementing discrete Gaussian Sampling over the new algebraic structure and a draft of the research paper for the proposed NTRU are expected in this phase. Start to implement the corresponding prototype. The design report is expected to cover the tailored new algebraic tools used in the new algebraic structure, corresponding to 56-bit, 80-bit, 128-bit and 256-bit security.
- Phase 5-6: Research and implement the proposed NTRU. A patent is also expected in this phase. A prototype is expected for provably secure NTRU on 56-bit security construction.

References

- [IEEE1363] IEEE P1363. Standard specifications for public-key cryptography. http://grouper.ieee.org/groups/1363/.
- [HS03] N. Howgrave-Graham, J. H. Silverman, A. Singer, and W. Whyte,"NAEP: provable security in the presence of deryption failures," IACR Cryptology ePrint Archive http://eprint.iacr.org/2003/172.
- [HS05] N. Howgrave-Graham, J. H. Silverman, A. Singer, and W. Whyte, "Choosing parameter sets for NTRUEncrypt with NAEP and SVES-3," in Pproceedings of The Cryptographers Track at the RSA Conference 200-CT-RSA 2005 (Lecture Notes in Computer Science). San Francisco, CA, USA: Springer-Verlag, 2005, vol. 3376, 2005, pp. 118-135.
- [PC09] R. A. Perlner and D. A. Cooper. Quantum resistant public key cryptography: a survey. In Proc. of IDtrust, pages 85_93. ACM, 2009.
- [SS11] D. Stehlé and R. Steinfeld, Making NTRU as Secure as Worst-Case Problems over Ideal Lattices, in: Proc. of EUROCRYPT, pp. 27–47, 2011.

[SS13] D. Stehlé and R. Steinfeld, Making NTRUEncrypt and NTRUSign as Secure as StandardWorst-Case Problems over Ideal Lattices, IACR Cryptology ePrint Archive 2013 (2013), http://eprint.iacr.org/2013/004.

Click here to back to the Top Page

HIRPO2017120303: Network layer security research on IoT with massive interconnection

1 Theme: Network & Information security Technology

2 Subject: Internet of Things Security

List of Abbreviations

IoT: Internet of Things

3 Background

Internet of Things (IoT) gradually evolve from connecting traditional vertical domains to cross-system and cross-service connection. More and more scenarios require cross-Internet communication and collaborations among massive devices in heterogeneous networks.

Although heterogeneous network connection has better ability and flexibility, it also becomes more vulnerable to attacks which bring two kinds of security requirements:

1、 Traditional Security Requirements: A study of solutions to traditional security requirements such as authentication and encryption in massive interconnected IoT networks

2、 New Security Requirements: A study of the new security threats and solutions to these threats in the new IoT application scenarios

Currently, there are few research works with focus on the security in network layer of the Internet of Things, but it will be more and more important

to the development of IoT because of the massive communication cross-internet.

4 Scope

1) Research on traditional security requirements IoT with massive interconnection

Secure Channel: Lightweight secure channel technology that can satisfy the requirements in low-power, high-mobility, massive interconnection IoT network. Control plane includes authentication methods and protocols, and data plane includes the encryption method and protocols instead of IPsec or improvement of it.

2) **Research on new security threats brought by new network architecture and corresponding defense strategy**

Threat Model: the most intelligent devices are human-related, mobile and intellective, these characteristics, means human malicious behavior can introduce new security threat models.

The defense methods include but not limited to:

(1) Trust Management：Each device may become the requester and provider of a service, and the dynamic judgment of the trusted degree of the node becomes an important consideration in selecting a service node.

(2) Privacy Protection: Future Internet requires users sharing their information in many scenarios. A security-sensitive scenario requires strategy to protect users' privacy while users sharing their informations.

5 Expected Outcome and Deliverables

Technical reports on lightweight secure channel technology.

Technical reports on security analysis on threat model and defense strategy

Related simulation platform with source codes and description

2~3 Invention/patents;

6 Acceptance Criteria

Project proposal is accepted by the evaluation team, Huawei.
Project deliverables are accepted by the evaluation team, Huawei.
Lightweight authentication and encryption method: Node energy consumption is lower than IPSec.

7 Phased Project Plan

Phase1 (~3 months): Survey the state of the art of securing Internet of Things with lightweight IPsec technology and provide the related technical report.

Phase2 (~6 months): Research on lightweight secure channel technology that can satisfy the low-power, high-mobility, massive interconnection IoT network. Provide the related technical report and patent.

Phase3 (~9 months): Survey the state of the art of security issue and defense method on new security threats bring by new network architecture

Phase3 (~12 months): Research on the technology on threat model and defense strategy. Provide the related technical report and patent.

Phase4 (~18months): Related simulation platform with source codes and description.

Click here to back to the Top Page

HIRPO2017120702: Research of automatic vulnerability discovery Project

1 Theme: Network & Information security technology

2 Subject: Automatic Vulnerability Discovery Technology

Project name: Research of automatic vulnerability discovery Project

List of Abbreviations

AI: Artificial Intelligence

ML: Machine Learning

AFL: American Fuzzy Lop

3 Background

Manually vulnerability discovery is a tedious and complicate task, especially in large-scale software development.Searching and implementing automatic vulnerability discovery is extremely necessary for large-scale software

Nowadays, security testing of large-scale software is mainly conducted with the help of black-box fuzzing. However, black-box fuzzing can only deduce based on the final output of the testing, which keeps it from being smart enough to understand the details of the program during the test. And this also leads to the common problem for black-box fuzzing, that is, it would soon reach a point where no new branches can be found and complex branches cannot be effectively tested.

In order to overcome the shortcomings of black-box fuzzing, intelligent fuzzing like AFL, and symbolic execution are developed for security testing. A

combination of these technologies can substantially improve the performance of security testing.

Combination of different technique of vulnerability discovery is a tradeoffs between completeness, speed, precision and scalability. How to improve the combination property is a topic researched continually.

4 Scope

1) Combination and optimization of existing vulnerability discovery technologies Including(points as following and other points unmentioned here):

1) The optimization of the efficiency of symbolic execution and intelligent fuzzing.

2) The combination of static analysis, taint analysis, fuzzing, and symbolic execution.

2) AI and ML(or other methods and techlogies) in vulnerability discovery: The research of AI and ML technology as an auxiliary component in vulnerability discovery.

5 Expected Outcome and Deliverables

1) Technical report of the optimizing existing vulnerability discovery technologies, including symbolic execution, intelligent fuzzing ,etc;

2) Technical report of AI as an auxiliary component of vulnerability discoverty.

3) related DEMO

4) 1-2 patents of invention.

6 Acceptance Criteria

1) 0-day vulnerability can be discovered in the middle size software;

2) Efficiency, precsion and coverage can be increased by at least 20% compared with the prior art.

7 Phased Project Plan

Phase1 (~1 months): Survey the state of the art of vulnerability discovery solutions and technologies, analyze and provide the related technical report.

Phase2 (~6 months):Research on optimizing of existed vulnerability discovery solutions and technologies (including static analysis, taint analysis, fuzzing, and symbolic execution, etc, and combination of them).

Phase3 (~5 months): Research and provide related algorithms, demo and experiment results and patents

Click here to back to the Top Page

HIRPO2017120703: Research of vulnerability discovery, attack detection and consolidation of virtualization platform

1 Theme: Network & Information security technology

2 Subject: Virtualization Security Technology

List of Abbreviations

VM：Virtual Machine

I/O：Input/Output

3 Background

Virtualization platform (i.e. Hypervisor) is the critical component of cloud based infrastructure.

Compared to the traditional architecture, the security of the virtualization platform is a special and important issue in the cloud architecture.

When the virtualization platform is attacked (for example, escape of vm, information leakage between host and vm) by malicious guests, the security of the entire cloud based business will be seriously affected.

How to implement an end-to-end vulnerability detection, attack inspection, and security consolidation of virtualization platform has been a hot topic.

Isolation based on resource sharing is the essence of virtualization. Inappropriate isolation mechanism and some fallacious implement of it will cause serious security problems.

Vulnerability of isolation mechanism will be exploited by attackers and attack detection is important for the operation of cloud based business.

Finally, we need to consolidate the virtualization platform to enhance the robustness and prevent the core data from being accessed when the intrusion attack towards virtualization platform was successful , etc.

4 Scope

1) **Methods of detection of Virtualization vulnerability:** Research on the method of vulnerability analysis and detection for resource sharing and isolation.

2) **Methods of detection of attacks of Virtualization platform:** Research on adopting AI and big data for methods of detection and analysis of key behaviors of VMs, such as I/O port. Build a model database of key behaviors for malicious action detection.

3) **Consolidation of Virtualization platform**：Research on the optimization of the virtualization isolation mechanism, and the protection of sensitive data after being attacked.

5 Expected Outcome and Deliverables

5) Report on the technologies detection of attacks on Virtualization platform.

6) Report on the consolidation of Virtualization platform.

7) Related DEMO

8) 1-2 patents of invention.

6 Acceptance Criteria

3) 0-day vulnerability can be discovered in the virtualization platform (including XEN，KVM Vmware，etc.);

4) Precision of detecting attack towards virtualization platform can not be lower than 85%.

5) The consolidation solution can prevent core data from being accessed in the process of attack towards virtualization platform (can be experimental verified).

7 Phased Project Plan

Phase1 (~1 months): Survey the state of the art of virtualization platform security solutions and technologies, analyze and provide the related technical report.

Phase2 (~6 months): Research on the technologies of vulnerability discovery, attack detection and consolidation of virtualization platform and provide the related technical report.

Phase3 (~5 months): Research and provide related algorithms, demo and experiment results and patents

Click here to back to the Top Page

HIRPO2017121101: Using Block-Chain technology to enhance cloud core network efficient

1 Theme: Network & Information security Technology

2 Subject: Block-Chain in Cloud Core Network

Project name: Using Block-Chain technology to enhance cloud core network efficient

List of Abbreviations

IoT	Internet of Things

3 Background

In 5G core network framework, 3GPP uses micro-service architecture to make the core network more agility and flexible. The block-chain technology is designed to be a security distributed database which can maintain a continuously growing list of ordered records. Will the block-chain technology be a good one to enhance the core network efficient? Is there some use case which is suitable to use block-chain technology is worthwhile to study, such as network safety and IoT.

4 Scope

- Survey on block-chain technology and its using in different domain.
- Research on how to using block-chain in cloud core network. Find certain use case (e.g. network safety, IoT, network function architecture) which is suitable to use block-chain technology and

design the network structure and data sharing model by using block-chain. Give an end-to-end solution.

- Prove the efficiencies of the model, design and finish a demo of the model for verification.

5 Expected Outcome and Deliverables

- 1 survey report
- 2 research report
- 1 demo design
- 1 patents

6 Acceptance Criteria

- A detailed deliverables in section 6

7 Phased Project Plan

Phase1 (~2 months): Survey of block-chain and its using in different domain.

Phase2 (~3 months): Research on using block-chain to build the IoT network structure and data sharing model. The research should give a end-to-end solution for the IoT equipment.

Phase3 (~5 months): Prove the efficiencies of the model and accomplish a demo to verify the practicability of the network structure and data sharing model.

Click here to back to the Top Page