NANYANG TECHNOLOGICAL UNIVERSITY

LATTICES IN CONSTRUCTIONS OF DENSE SPHERE PACKINGS AND CERTAIN CRYPTOGRAPHIC SCHEMES

SHANTIAN CHENG

SCHOOL OF PHYSICAL AND MATHEMATICAL SCIENCES

2016

LATTICES IN CONSTRUCTIONS OF DENSE SPHERE PACKINGS AND CERTAIN CRYPTOGRAPHIC SCHEMES

SHANTIAN CHENG

SHANTIAN CHENG

SCHOOL OF PHYSICAL AND MATHEMATICAL SCIENCES

A thesis submitted to the Nanyang Technological University
in partial fulfilment of the requirement for the degree of
Doctor of Philosophy

2016

I dedicate this thesis

in token of affection and gratitude

to my beloved parents

Guangmin Cheng, Bo Xu,

and fiancee

Yujie Nan.

ACKNOWLEDGEMENTS

First of all, I would like to express my deep gratitude to my supervisors, Prof. San Ling and Prof. Chaoping Xing, for their invaluable guidance and encouragement during my PhD studies. It is a great privilege for me to accomplish my PhD studies under their supervision and support. They are tremendous role models for me to learn, not only in academia but also in daily life. As their student, I will try my best to live up to their expectations and achieve more success in the future.

I am much grateful to the collaborators in my two papers in cryptography, Dr. Ta Toan Khoa Nguyen, Prof. Huaxiong Wang, and Juanyang Zhang for their precious help and support. A special thank you goes to Dr. Ta Toan Khoa Nguyen, since the cooperation with him is really a valuable experience, from which I gained a lot of knowledge in cryptography and abilities in team coordination. In addition, I wish to express my sincere gratitude to Dr. Hyung Tae Lee for his generous help in my revision of the ISPEC'15 paper, and Ivan Tjuawinata for the helpful discussions on C++ implementation of some encryption schemes.

It is also a good opportunity for me to express my appreciation and thanks to all the anonymous reviewers, who have offered great help, advice and comments on my PhD research results. I sincerely admire their profound knowledge and rigorous scientific attitude in research, and I believe their precious advice have helped improve my results.

Furthermore, I would like to gratefully thank Dr. An Yang, Dr. Anderson Siang Jing Yeo, Dr. Guizhen Zhu for their generosity in offering valuable advice in career

planning and sharing their experience in job hunting. Their genuine help offers me a broader understanding of the future career of a PhD holder.

My deepest gratitude goes to my parents, Guangmin Cheng and Bo Xu. Although they totally could not understand what I am doing everyday and I have even lost my temper several times over the phone when I was caught in deep depression and stress, they still provide unending encouragement, support and patience, which have accompanied me throughout my studies.

I am deeply indebted to my fiancee, Yujie Nan for her unwavering love. I would never have been able to finish my PhD studies without her unconditional support. She is the one for me to have and to hold. She is the reason for me to be happy, strong and positive in life. With the submission of this thesis, we can finally bring an end to the long-distance engagement and put the wedding on the agenda. It is so inspiring to conceive the image that we strive together for our common better future that I can hardly wait.

Finally I have to thank Euclid for his "τριώβολον (three pence)".

ABSTRACT

In this thesis we concentrate on the usage of lattices to construct explicit sphere packings with high density, packing families with good asymptotic properties, and cryptographic schemes with special functionalities, including (delegatable) policy-based signature and revocable identity-based encryption.

First we introduce new methods using codes and lattices from number fields to construct dense packings in Euclidean spaces. Let $\omega = (-1 + \sqrt{-3})/2$. For any lattice $P \subseteq \mathbb{Z}^n$, $\mathcal{P} = P + \omega P$ is a subgroup of $\mathcal{O}_K^n$, where $\mathcal{O}_K = \mathbb{Z}[\omega] \subseteq \mathbb{C}$. As $\mathbb{C}$ is naturally isomorphic to $\mathbb{R}^2$, $\mathcal{P}$ can be regarded as a lattice in $\mathbb{R}^{2n}$. Let P be a multiplicative lattice (principal lattice or congruence lattice) introduced by Rosenbloom and Tsfasman. We concatenate a family of special codes with $t_{\mathfrak{P}}^{\ell} \cdot (P + \omega P)$, where $t_{\mathfrak{P}}$ is a generator of a non-zero prime ideal $\mathfrak{P}$ of $\mathcal{O}_K$. Applying this concatenation to a family of principal lattices, we obtain a new family with asymptotic density exponent $\lambda \geqslant -1.26532182283$, which is better than -1.87 given by Rosenbloom and Tsfasman by considering only principal lattice families. For a new family based on congruence lattices, the result is $\lambda \geqslant -1.26532181404$, which is better than -1.39 obtained by considering only congruence lattice families.

More generally, via the canonical $\mathbb{Q}$-embedding of arbitrary number field K into $\mathbb{R}^{[K:\mathbb{Q}]}$, both the prime ideal $\mathfrak{p}$ and its residue field κ can be embedded as discrete subsets in $\mathbb{R}^{[K:\mathbb{Q}]}$. Thus we can concatenate the embedding image of the Cartesian product of n copies of $\mathfrak{p}$ together with the image of a length n code over κ. This

concatenation leads to a packing in the Euclidean space $\mathbb{R}^{n[K:\mathbb{Q}]}$. Moreover, we extend the single concatenation to multiple concatenations to obtain dense packings and asymptotically good packing families. For instance, with the help of Magma, we construct a 256-dimensional packing denser than the Barnes-Wall lattice BW_{256}.

Next we develop the recent techniques in lattice-based cryptography to construct a (delegatable) policy-based signature scheme and a revocable identity-based encryption scheme from lattice assumptions. Policy-based signature, introduced by Bellare and Fuchsbauer at PKC 2014, is a new type of digital signature in which a signer is only allowed to sign messages satisfying certain policy specified by the authority, but the signatures should not reveal the underlying policy. We adapt Langlois et al.'s zero-knowledge argument system (PKC 2014) for the Bonsai tree signature scheme (Eurocrypt 2010) to enable the prover to convince the verifier that its secret witness satisfies an additional condition. Making the protocol non-interactive via the Fiat-Shamir transformation, we obtain a policy-based signature scheme supporting polynomially many policies, which satisfies the two security requirements (simulatability and extractability) in the random oracle model. Furthermore, our construction can be efficiently extended to a delegatable policy-based signature, thanks to the hierarchical structure of the Bonsai tree.

In view of the expiration or revelation of the user's private credential (or private key) in a realistic scenario, identity-based encryption (IBE) schemes with an efficient key revocation mechanism, or for short, revocable identity-based encryption (RIBE) schemes, become prominently significant. We present an RIBE scheme from lattices by combining two Agrawal et al.'s IBE schemes (Eurocrypt 2010) with the subset difference method. In particular, our scheme may serve as a solution to a question posed by Chen et al. (ACISP 2012).