格基环签名简介

Kurt Pan

Fudan University

June 24, 2021

Outline

Section 1

基于 ws-NIZK 证明系统的环签名方案

基于 MV03 和 FSwA 的环签名方案

- 基于 ws-NIZK 证明系统的格基环签名方案可以分为两个阶段. 早期方案使用的 ws-NIZK 证明系统为 *MV03 证明系统*[1] 和 *Fiat-Shamir-with-Abort(FSwA) 证明系统*[2]. 这两个证明系统最早被用于证明 GapCVP 或非齐次最小整数解问题 (inhomogeneous small integer solution, ISIS) 等格上困难问题, 应用到环签名的构造时需要配合额外的技术, 效率较低.
- 2018 年后的部分格基环签名方案发展了新的 ws-NIZK 证明系统, 包括 one-out-of-many 的证明系统 ESS+19 和 ESL+19 (适用于自组织的群成员关系证明). 这些新型证明系统极大提升了格基环签名的实际效率, 达到或接近了实用化需求.

[1] Daniele Micciancio and S. Vadhan. "Statistical Zero-Knowledge Proofs with Efficient Provers: Lattice Problems and More". In: *CRYPTO*. 2003.

[2] Vadim Lyubashevsky. "Lattice Signatures Without Trapdoors". In: *IACR Cryptol. ePrint Arch.* 2011.

基于 MV03 和 FSwA 的环签名方案

- MV03 证明系统是由 Micciancio 和 Vadhan 于 CRYPTO 2003 提出的零知识证明系统，可以证明 GapCVP 等格上最坏情况的困难问题.
- FSwA 证明系统由 Lyubashevsky 于 Asiacrypt 2009 和 Eurocrypt 2012 提出并发展, 其设计思想与基于离散对数的 Schnorr 协议类似, 它允许证明者证明自己持有 ISIS 问题的证据, 即持有某个短向量 x 满足 $A \cdot x = y (\mathrm{mod} q) \wedge \|x\| \leq \beta$, 其中 A 和 y 为公开的矩阵或向量, β 是公开的数值.
- MV03 证明系统的单次执行允许恶意证明者以 $1/2$ 的概率欺骗验证者 (soundness error 等于 $1/2$), 因此需要至少 λ 次重复执行协议才能保证恶意证明者成功欺骗的概率是可忽略的 (λ 为安全参数), 效率较低.
- FSwA 证明系统单次执行即可保证 soundness error 为可忽略的, 效率明显优于 MV03.

基于 MV03 和 FSwA 的环签名方案

- MV03 和 FSwA 证明系统只能满足弱可靠性，即证明者对自己持有短向量 x 满足 ISIS 的实例 (A, y, β) 的证明，实际上只能确保证明者知道 $\|x'\| \leq \beta'$ 满足 $A \cdot x' = cy$，其中 $\beta' > \beta, c > 1$.
- FSwA 的这一缺点也进一步限制了它在证明密文正确性等需要精确的可靠性场景下的使用. 受限于 MV03 和 FSwA 可证明的语言类型，相应的环签名方案只能做到签名大小与环的规模线性相关.

基于 MV03 和 FSwA 的环签名方案

- 早期的格基环签名方案可以视作是经典的 CDS 机制在格密码中的应用.
- CDS 机制是指 Cramer、Damgård 和 Schoenmakers[3] 于 CRYPTO 1994 上提出的一种按照 OR 关系组合 Sigma 协议机制.
- 具体的, 若对于某个 NP 语言 $\mathcal{L}$, 存在满足特定条件的协议 Σ 可以证明 $x \in \mathcal{L}$, 那么经由 CDS 机制可以得到一个新的协议 Σ^{OR} 来证明 $x_1 \in \mathcal{L} \vee \cdots \vee x_N \in \mathcal{L}$.
- 如果 Σ 协议是身份认证协议, 则 Σ^{OR} 可经过 Fiat-Shamir 转换得到环签名方案。
- 使用 CDS 机制，Melchor 等人[4]将基于 FSwA 的格基身份认证协议转换为环签名方案. 该环签名方案和所有经由 CDS 机制构造的环签名方案一样, 签名大小和环的规模线性相关.

[3] R. Cramer, I. Damgård, and Berry Schoenmakers. "Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols". In: *CRYPTO*. 1994.

[4] C. A. Melchor et al. "Adapting Lyubashevsky's Signature Schemes to the Ring Signature Setting". In: *AFRICACRYPT*. 2013.

基于 FSwA 的可链接环签名方案

- Baum、Lin 和 Oechsner 的方案[5] 与 Torres 等人的方案[6]类似，可以视作是基于离散对数的可链接环签名方案在格上的迁移. 首先设计 FSwA 协议，证明用于实现链接性的向量是用签名者的私钥诚实生成的，再利用 CDS 机制隐藏签名者的公钥，经由 Fiat-Shamir 转换后形成可链接环签名. 这两个方案签名大小和环的规模成线性关系，主要应用是匿名数字货币等环规模较小的场景.
- 这两个方案所实现的可链接性为一次可链接性，即任意两个由同一私钥产生的签名可以被公开链接. 一次可链接性与标准的基于标签 *(Tag-based)* 的可链接性有严格的区别. 从应用角度，一次可链接性足够匿名数字货币的使用需求. 从技术角度，实现基于标签的可链接性需要引入伪随机函数作为组件，并用零知识证明系统来保证伪随机函数的正确执行. 这样的证明任务难以通过 FSwA 完成.

[5] Carsten Baum, H. Lin, and Sabine Oechsner. "Towards Practical Lattice-Based One-Time Linkable Ring Signatures". *IACR Cryptol. ePrint Arch.* 2018.

[6] Wilson Abel Alberto Torres et al. "Post-Quantum One-Time Linkable Ring Signature and Application to Ring Confidential Transactions in Blockchain (Lattice RingCT v1.0)". In: *IACR Cryptol. ePrint Arch.* 2018 (2018), p. 379.

ESS+19 和 ESL+19 的环签名方案

- 经典密码体制下 Groth 和 Kohlweiss[7] 设计基于离散对数困难问题设计了签名大小与环的规模成对数关系的环签名方案.
- 该环签名方案的核心构造是一种新的 *one-out-of-many* 零知识证明协议: 证明 N 个承诺 $\{c_i\}_{i\in[N]}$ 的某个承诺值的消息为 0 .
- FSwA 证明系统与基于离散对数的 Schnorr 协议的相似性揭示了将更多的基于离散对数的协议迁移到格基协议的可能, 也启发研究人员思考如何利用 Groth 和 Kohlweiss 的设计方法来构造高效格基环签名.

[7] Jens Groth and Markulf Kohlweiss. "One-Out-of-Many Proofs: Or How to Leak a Secret and Spend a Coin". In: *IACR Cryptol. ePrint Arch.* 2014 (2014), p. 764.

ESS+19 和 ESL+19 的环签名方案

- 在 ACNS 2019 上, Esgin 等人[8]解决了将 Groth 和 Kohlweiss 设计思想迁移到格上的若干问题, 设计了基于模格上的 SIS 问题的 one-out-of-many 协议, 并构造了具有对数级签名大小的环签名方案 ESS+19.
- 该 one-out-of-many 协议的 soundness error 为 1/poly, 需要多次重复执行协议才能实现可忽略的 soundness error.

[8] Muhammed F. Esgin et al. "Short Lattice-based One-out-of-Many Proofs and Applications to Ring Signatures". In: *IACR Cryptol. ePrint Arch.* 2018.

ESS+19 和 ESL+19 的环签名方案

- 在 CRYPTO 2019 上, Esgin 等人[9]实现了单次执行即可保证可忽略的 soundness error. 他们将该证明技术提炼为适用于非线性多项式关系的零知识证明技术, 并发展了基于环中国剩余定理的批处理技术, 进一步降低此类零知识证明的通信复杂度，提高效率。
- 利用这一新型技术对他们之前提出的环签名方案进行了重构, 得到了基于模格上困难问题的环签名方案 ESL+19.
- 对 2^{10} 规模的环, 该方案的签名大小仅为 100 KB 左右, 是目前适用于大规模环的效率最高的后量子安全环签名方案.

[9] Muhammed F. Esgin et al. "Lattice-based Zero-Knowledge Proofs: New Techniques for Shorter and Faster Constructions and Applications". In: *IACR Cryptol. ePrint Arch.* 2019.

Section 2

基于 ss-NIZK 证明系统的环签名方案

基于 ss-NIZK 证明系统的环签名方案

- 现有基于格的 ss-NIZK 证明系统包括 Stern 类协议和 YAZ+19 证明系统. Stern 类协议和 YAZ+19 证明系统的通用性强, 可以证明格密码学中常见的一大类语言, 可以构造环签名的各种功能变种.
- 但 Stern 类协议单次执行的 soundness error 为 2/3, 需要多次重复执行才能实现可忽略的 soundness error, 根本上限制了基于 Stern 类协议的环签名的效率.
- YAZ+19 可以视作 Stern 类协议的改进版本, 单次执行的 soundness error 为多项式的逆, 需要重复执行的次数显著降低.
- 二者都无法通过单次执行实现可忽略的 soundness error, 在特定应用上效率明显低于某些 ws-NIZK 证明系统.

基于 Stern 类协议的环签名方案

- Stern 类协议最早由 Stern[10] 提出并用于设计基于编码理论的身份认证协议，而后被 Tanaka 和 Xagawa[11] 引入到格密码学中用于构造基于格的身份认证协议.
- Ling 等人[12]改进了 Kawachi 等人的工作, 使得 Stern 类协议可以“精确地” 证明 ISIS 问题 (与 FSwA 不同).
- 此后, Stern 类协议被广泛地用于设计基于格的环签名方案, Stern 类协议的设计技巧也在应用中不断发展.
- 目前 Stern 类协议可以证明符合如下形式的 NP 关系: $R_S := \left\{\left(A \in \mathbb{Z}_q^{n\times d}, v \in \mathbb{Z}_q^n, \mathbb{V} \subset \{-1,0,1\}^d\right); x : A \cdot x = v \bmod q, x \in \mathbb{V}\right\}$.

[10] J. Stern. “A new paradigm for public key identification”. In: *IEEE Trans. Inf. Theory* 42 (1996), pp. 1757–1768.

[11] A. Kawachi, Keisuke Tanaka, and Keita Xagawa. “Concurrently Secure Identification Schemes Based on the Worst-Case Hardness of Lattice Problems”. In: *ASIACRYPT*. 2008.

[12] S. Ling et al. “Improved Zero-Knowledge Proofs of Knowledge for the ISIS Problem, and Applications”. In: *Public Key Cryptography*. 2013.

基于 Stern 类协议的环签名方案

- 在 Eurocrypt 2016 上, Libert 等人[13] 基于 Stern 类协议设计了签名大小与环规模成对数关系的环签名方案, 解决了格基紧致环签名构造这一公开难题.
- 在经典密码体制下, 紧致的环签名方案通常需要依赖累加器这种特殊结构. 累加器可以视作是对集合的承诺方案, 且具备紧致的成员关系证明方式. 已知的累加器分为三类, 包括基于 Strong RSA 假设的累加器, 基于双线性对的累加器, 以及基于 Merkle 树的累加器.
- Libert 等人使用基于 SIS 困难问题的杂奏函数构建了 Merkle tree 作为基于格的的累加器方案, 再针对该累加器设计了 Stern 类型的零知识证明协议. 对于 Merkle tree 中的叶子节点, 它到根节点的路径可以作为该叶子节点属于该 Merkle tree 的证据, 而该证据的大小和叶子节点的总数成对数关系. 这也是 Libert 等人的方案可以实现对数级签名大小的根本原因.

[13] Benoît Libert et al. "Zero-Knowledge Arguments for Lattice-Based Accumulators: Logarithmic-Size Ring Signatures and Group Signatures Without Trapdoors". In: *EUROCRYPT*. 2016.

基于 Stern 类协议的环签名方案

- Stern 类协议作为核心组件被用于设计一些环签名的变种方案.
- Yang 等人[14] 在 Libert 等人提出的格基环签名方案基础上设计了基于格的可链接环签名方案.
- 在 CT-RSA 2020 上, Feng 等人[15]提出了可追踪环签名的通用设计框架, 并基于 Stern 类协议构造了格基可追踪环签名方案

[14] R. Yang et al. "Lattice-Based Techniques for Accountable Anonymity: Composition of Abstract Stern's Protocols and Weak PRF with Efficient Protocols from LWR". In: *IACR Cryptol. ePrint Arch.* 2017 (2017), p. 781.

[15] Hanwen Feng et al. "Traceable Ring Signatures with Post-quantum Security". In: *CT-RSA*. 2020.

基于 YAZ+19 证明系统的环签名方案

- 在 CRYPTO 2019 上, Yang 等[16]提出了一种新的格基零知识证明系统 YAZ+19.
- 功能方面, 证明系统与 Stern 类协议接近, 可以证明格密码学中常见的一大类 NP 语言, 并具备标准的可靠性.
- 效率方面, 该证明系统单轮执行的 soundness error 仅为 $1/\text{ poly}$, poly 代表安全参数的多项式. 该数值小于 Stern 类协议的 soundness error $2/3$, 将 soundness error 降低到可忽略的大小所需要的重复次数也随之少于同等安全参数下 Stern 类协议所需重复次数, 因此该证明系统效率较 Stern 类协议有显著提升.

[16] R. Yang et al. "Efficient Lattice-Based Zero-Knowledge Arguments with Standard Soundness: Construction and Applications". In: *IACR Cryptol. ePrint Arch.* 2019.

基于 YAZ+19 证明系统的环签名方案

- YAZ + 19 证明系统设计上结合了 FSwA 和 Stern 类协议的优点. 对于需要证明的 ISIS 问题 $(A, y; \mathrm{x})$, 该证明系统首先采用类似于 FSwA 的方式, "宽松地" 证明存在向量 x' 满足 $A \cdot x' = cy \bmod q$, 再采用类似于 Stern 类协议的方式"精确地" 证明存在向量 $x \in \{-1, 0, 1\}^n$ 满足 $x' = cx$. 结合两者的优点, YAZ + 19 实现了精确证明和更小的 soundness error.
- Yang 等人使用该证明系统对基于 Stern 类协议的环签名方案进行了全面的升级, 得到的环签名方案是目前基于标准格效率最优的方案.

Section 3

基于变色龙 Hash 的环签名方案

基于变色龙 Hash 的环签名方案

- 在 ACNS 2019 上, Lu、Au 和 Zhang[17]提出了适用于小规模环的实用格基环签名方案 Raptor. 与第三代的其他工作不同, Raptor 取得的效率提升并非是来源于新型零知识证明协议, 而是来源于环签名方案的新设计框架.
- Lu 等人深入分析了 Rivest、Shamir 和 Tauman 提出第一个环签名通用构造框架 RST01, 提炼出了 RST01 框架实际上所需要的密码组件, 即*增强变色龙杂凑函数 (chameleon hash plus, CH+)*.
- 他们基于标准格和 NTRU 格分别构造了 CH+, 并在此基础上构造了格基环签名方案.
- 与 RST01 框架的其他环签名一样, Lu 等人的方案中签名大小与环的规模线性相关, 因此更适用于小规模环的情况. 他们的实现测试结果说明该方案对于规模较小的环 (例如由 5 个公钥构成的环) 效率可以满足实用需求 (对应签名大小为 6.3 KB).

[17] Xingye Lu, M. Au, and Zhenfei Zhang. "Raptor: A Practical Lattice-Based (Linkable) Ring Signature". In: *IACR Cryptol. ePrint Arch.* 2018 (2018), p. 857.

- Lu 等人也提出了一种新的一次可链接环签名设计方法. 他们的方案区别于 Franklin 和 Zhang 提出的构造方法, 通过在环签名中附加一次性签名的方法来实现同一私钥产生的不同签名的可链接性.
- Wang、Chen 和 Ma[18] 总结并推广了此种可链接环签名设计技巧.

[18] Xueli Wang, Y. Chen, and Xuecheng Ma. "Adding Linkability to Ring Signatures with One-Time Signatures". In: *ISC*. 2019.

Section 4

标准模型下的环签名方案

标准模型下的环签名方案

- Brakerski 和 Kalai[19] 提出了一种高效的通用框架来构造标准模型下的环签名方案. 该文献定义了环陷门 *(ring trapdoor)* 函数, 并展示了如何利用环陷门来构造环签名. 环陷门函数是对普通陷门函数的扩展, 它不仅要求给定 f 和 y 找到 x 使得 $f(x) = y$ 是困难的, 也要求对于给定的 $f_1, \cdots, f_t, y$ 来找到 $x_1, \cdots, x_t$ 使得 $\sum_{i=1}^{t} f_i(x_i) = y$ 是困难的; 但如果具有任何一个 f_i 对应的陷门, 则可以有效计算出所有满足条件的 $x_1, \cdots, x_t$. 运用环陷门函数构造环签名方案的思路也比较直观, 函数本身作为签名的公钥, 函数对应的陷门作为签名的私钥, 求出的逆 $x_1, \cdots, x_t$ 作为环 $f_1, \cdots, f_t$ 下的签名.

[19] Zvika Brakerski and Y. Kalai. "A Framework for Efficient Signatures, Ring Signatures and Identity Based Encryption in the Standard Model". In: *IACR Cryptol. ePrint Arch.* 2010 (2010), p. 86.

标准模型下的环签名方案

- 对于环陷门函数这一新定义，该文献基于格上的最小整数解 (short integer solution, SIS) 问题和双线性对上的计算性 Diffie-Hellman 问题分别构造了具体的环陷门函数. 使用基于 SIS 问题的环陷门函数实例化通用框架可以得到在标准模型下可证安全的格基环签名方案. 由于该方案中，签名由所有的逆组成，因此签名的大小和环的规模线性相关. 同时，基于格的环陷门函数依赖格的陷门函数，该陷门函数需要较大的格维度，这也导致签名的实际大小过大，不满足实际应用需要.

Section 5

基于后量子安全通用 NIZK 证明协议的环签名方案

基于后量子安全通用 NIZK 证明协议的环签名方案

- 环签名的构造通常依赖于 *NIZK 证明系统*或*两轮证据不可区分证明系统 (ZAP)*. 然而在标准模型, 包括*共享字符串模型 (common reference string model, CRS)* 和*朴素模型 (plain model)* 中, 高效 NIZK 证明系统和 ZAP 的已知构造方式非常有限, 主要为 Groth 和 Sahai[20]利用*双线性映射*构造的证明系统.
- Groth 和 Sahai 的证明系统也是现有的在标准模型下可证安全的环签名方案的构造基础. 如何基于抗量子的困难问题假设构造类似于 Groth 和 Sahai 的 NIZK 证明系统目前是一个公开难题.

[20] Jens Groth and A. Sahai. "Efficient Non-interactive Proof Systems for Bilinear Groups". In *EUROCRYPT*. 2008.

基于后量子安全通用 NIZK 证明协议的环签名方案

- 理论上可证明所有 NP 语言的通用 *NIZK* 证明系统或者 ZAP 可以用于证明格密码学和对称密码学相关的语言. CRS 模型下的通用 NIZK 证明系统构造是一个非常经典的问题, 早在 FOCS 1990 上 Feige, Lapidot 和 Shamir[21] 就已经提出了基于单向陷门置换 *(one-way trapdoor permutation)* 的通用 NIZK 证明系统.
- 单向陷门置换可以基于大整数分解假设构造, 但我们对它的其他构造方式尤其是基于抗量子假设的构造方式却知之甚少, 这也使得后量子安全的通用 NIZK 证明协议是长期以来的公开难题.

[21] U. Feige, D. Lapidot, and A. Shamir. "Multiple non-interactive zero knowledge proofs based on a single random string". In: *Proceedings [1990] 31st Annual Symposium on Foundations of Computer Science* (1990), 308–317 vol.1.

基于后量子安全通用 NIZK 证明协议的环签名方案

- 可喜的是, 近年来对 Fiat-Shamir 转换在标准模型下的构造方法研究取得了突破性进展.
- CRYPTO 2019 上, Piekert 和 Shehian[22]基于 LWE 假设构造了具有 *Correlation Intractability (CI)* 性质的 Hash 函数, 该 Hash 函数可以用于替换 Fiat-Shamir 转换中的随机预言机, 从而得到 *CRS* 模型下的通用 *NIZK* 证明系统;
- Eurocrypt 2020 上, Badrinarayanan 等人[23]同样利用具有 CI 性质的 Hash 函数, 构造了基于 LWE 假设的 ZAP .
- 根据环签名的通用构造, 上述抗量子的证明系统也从理论上解决了标准模型下后量子安全环签名构造问题.
- 在实际效率方面, 基于 LWE 的具有 CI 性质的 Hash 函数构造复杂, 依赖于全同态加密等高级密码学原语, 目前距离实用化还存在非常巨大的差距.

[22] Chris Peikert and Sina Shiehian. "Noninteractive Zero Knowledge for NP from (Plain) Learning With Errors". In: *IACR Cryptol. ePrint Arch.* 2019 (2019), p. 158.

[23] S. Badrinarayanan et al. "Statistical ZAP Arguments". In: *IACR Cryptol. ePrint Arch.* 2019.

Thanks!