分布式密码的体系结构和研究内容

王　磊　　祝跃飞

（解放军信息工程大学信息工程学院网络工程系　郑州　450002）

摘　要：通过分析分布式密码各部分的历史渊源和相互联系，给出了分布式密码的体系结构，并对系统模型进行了较为完整的描述。结合密码学研究的基本思路和分布式密码的现状，指出了分布式密码的研究内容。

关键词：密码学，分布式密码，体系结构，研究内容

中图分类号：TN918.1　　**文献标识码**：A　　**文章编号**：1009-5896(2005)01-0146-04

Framework and Researching Content of Distributed Cryptography

Wang Lei　　Zhu Yue-fei

(*Dept of Network Eng., Institute of Information Eng.,*

Information Engineering University, Zhengzhou 450002, *China*)

Abstract　Framework of distributed cryptography is presented based on its development and relations among its branches. A systematical model of distributed cryptography is described at the same time. And researching content of distributed cryptography is reviewed based on researching principles of cryptography and status of distributed cryptography.

Key words　Cryptology, Distributed cryptography, Framework, Researching contents

1　概述

现实中有许多关键的控制或权利，如果交由单个人掌管，首先可能会由于掌控者主观滥用权力或控制权被攻击者得到而影响安全性，其次可能会由于掌控者主观不履行职责或控制权被破坏而使系统无法使用。如果简单地将控制权同时交给多人，虽然提高了可用性，但却降低了安全性。现实中常将这些控制分布式实现，如银行保险库需要三个保管员中至少两个同时提供密码才能开启。这些类似的分布式处理，能够同时提高安全性和可用性。

密码学的任务是为各种应用提供能有效保障安全的密码工具，为实现将各种关键控制进行某种分布式实现而提供的密码工具，自然地被称为分布式密码。现实中显然或实质是这类问题的应用比比皆是，对分布式密码提出了广泛而迫切的需求，分布式密码因而早已成为密码学研究的一大热点。

虽然经过了很长时间的深入研究，分布式密码一直没有明确的定义或描述，学术界通常只是将与之相关的秘密共享、可验证秘密共享、多方安全计算、门限密码等泛泛都看成分布式密码，而这些内容相互间又都有一定联系，这样，分布式密码就显得非常杂乱。

2003-07-25 收到，2004-04-12 改回
国家自然科学基金(90204015)资助项目

本文在分析各部分历史渊源和相互联系基础上，给出了十分明晰的分布式密码体系结构，并对系统模型进行了较为完整的描述。然后结合密码学的基本研究思路和分布式密码现状，指出分布式密码的研究内容。

2　分布式密码的体系结构

2.1 历史渊源与相互联系

2.1.1 *秘密共享*　1979 年，Shamir[1]和 Blakley[2]分别独立提出了秘密共享（Secret Sharing，SS）的概念和一类特殊共享的实现：一个秘密被分成 n 个份额，分别交由 n 个不同的分享者掌握，对一个固定的 $t \le n$，任意不少于 t 个份额可以构造出原来秘密，而任意少于 t 个份额得不到原来秘密的任何信息，被称为 (t,n) 门限秘密共享。

1987 年，Ito 等将门限推广到一般访问结构[3]。记分享者集合为 P，对 P 的子集合 A，如允许 A 中用户一起可以恢复秘密，称 A 为授权子集，否则称为禁止子集。所有授权子集的集合记为 Γ，所有禁止子集的集合记为 Δ，如果 $\Gamma \cap \Delta$ 为空集，则称（Γ，Δ）为一访问结构。

此后，各种分布式实现都首先考虑门限情形，进而考虑一般访问结构情形。另外，一些特殊的访问结构如通常管理

体制中的分级控制因具有一定现实意义而常被专门研究。

从门限到一般及一些特殊的访问结构，是分布式密码“分布式角度”的一条线索。

2.1.2 门限密码与分布式密码　1987 年，Desmedt 提出了面向团体的密码问题[4]，一个组织对外有一个固定的公钥，内部成员分享解密和签名的权利，一般认为是严格意义下分布式密码的提出。下面以分享签名权为例说明 Desmedt 提出的思路，将私钥分享后，各分享者由其份额分别得到一个部分签名，作为完整签名的份额，然后在不需要重构密钥条件下，由满足一定要求（如门限）的签名份额构造出完整的签名，当然前提是由达不到要求的签名份额得不到完整的签名，而且重构算法不泄露私钥及其份额的信息。

随后，Desmedt 和 Frankel 给出了基于 Shamir 门限共享和 ElGamal 加密的门限加密体制的实现[5]，并提出门限签名可类似实现的思路，门限密码由此兴起。将访问结构推广到一般情形，则自然形成了一般分布式密码的概念。鉴于分布式控制的优点，自然地从加密和签名的分布化扩展到各种可能的密码操作或功能的分布式实现，如分布式密钥生成、分布式密钥分发、分布式承诺、分布式认证等等逐渐被提出和实现。同时，许多多方安全应用如拍卖、投标等，其中具有一些地位等同的参与方，他们的许多操作可以视为或转化为某一集中实现密码功能或操作的分布式处理，自然归入分布式密码应用。

考虑各种集中式密码操作或功能的分布式实现，是分布式密码“密码角度”的另一条线索。

2.1.3 可验证秘密共享与安全多方计算　在基本的秘密共享体制中，如果分发或重构中有人提供了错误份额，则不能正确恢复共享的秘密。为此，1985 年 Chor 等提出了可验证秘密共享（Verifiable Secret Sharing, VSS）的概念[6]，基本思想是对份额附加某种一致性信息，从而可以检验份额的有效性，再辅以相关手段约束提供错误份额的行为。

1982 年，Yao 提出安全多方计算（Secure Multi-Party Computation, SMPC）概念[7]，即多个参与方在输入保密条件下正确计算约定函数值的问题。在后来的研究结果中，SMPC 实质上主要通过以下方式实现，首先各方将其输入在参与者中共享，然后使用相应的份额进行计算，分别得到正确结果的份额，最后由结果的份额恢复出结果。同时，为使各种份额合法从而计算正确，必然使用 VSS，这就使得 VSS 成为 SMPC 的关键工具[8, 9]。

而更重要的是，SMPC 研究中根据对攻击者计算能力的假设、攻击的方式及系统的物理信道等参量定义了分布式环境中的各种攻击模型（将在 2.3.3 节具体描述）。SMPC 首先探讨各种攻击模型下安全计算方案的存在性和理论构造问题。显然，各种分布式密码都可视为某种安全多方计算，必须同样考虑 SMPC 定义的攻击模型。这样，SMPC 的理论成果可能可以用来指导对应分布式密码的设计。SMPC 还研究各类具体函数的分布式计算实现，这些可能正是实现分布式密码特别是其中的各种分布式算法所需要的工具。虽然也有自身的一些理论和内容，但因与分布式密码联系如此紧密，SMPC 也被归入分布式密码。

考虑分布式环境中的各种攻击模型，可以看作是分布式密码的第三条线索。

2.2 分布式密码的体系结构

基于以上历史渊源和相互联系分析，我们认为，分布式密码研究分布式环境中各种攻击模型下各种集中式密码操作或功能在各种访问结构下的分布式实现。将以上 3 条线索形式化为如图 1 所示“三维空间”，我们给出分布式密码的体系结构，可以比较清晰地描述出其主要内容。而其他内容基本上与某种攻击模型相关，将在后面适当时机给出。

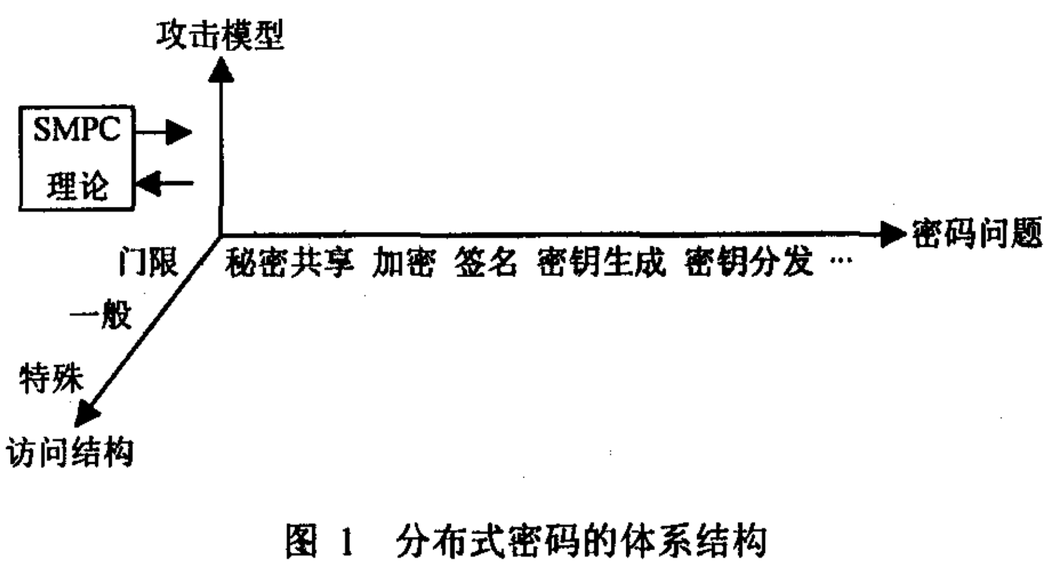

图 1　分布式密码的体系结构

2.3 分布式密码的系统模型

2.3.1 系统成员　一般称 n 个对等的参与者（人或服务器）为用户，用户对系统的控制由访问结构描述。

考虑一个外部攻击者，假设其有拉拢或攻破部分用户的能力，则包含内部串谋的情形。称被拉拢或攻破的用户为不诚实用户，未被拉拢或攻破的用户为诚实用户。

最好的密码协议当然是不用可信中心（Trusted Center, TC），但却不一定总能实现。通常先简单考虑使用 TC 承担必不可少的如系统初使化工作，进而努力设计分布式协议取代之，如果不能实现，则考虑类同 VSS 那样对其行为做一定约束使其辅助完成协议。

2.3.2 通信信道假设　首先，假设用户两两之间具有通信信道。部分信道现实中较少，且满足一定条件的部分信道总可以通过一些协议模拟成两两之间有通信信道的情形[10]，故不予考虑。在需要时合理假设用户已通过 PKI（Public Key Infrastructure）拥有了公钥系统及通过可信第三方或密钥协商协议实现了两两之间对称体制密钥分发，从而两两间可以实现可认证的保密通信。

其次，需要时假设存在一个广播信道以简化系统设计，此时任一用户可以向其余所有用户广播消息，保证所有合法用户收到消息一致。安全广播信道是分布式密码实现的重要

基础，因而，在点对点信道上实现安全广播信道的广播协议研究是分布式密码的一项内容。

在TC存在时，合理假设其与各个用户间有可认证的保密信道且可以使用广播信道（接收或发送消息）。

假设攻击者不能删除信道上传送的消息，因已经不属于密码学的研究内容。攻击者伪造消息和修改信道上传送的消息的行为，认为可以通过消息认证有效解决也不予考虑。

2.3.3 攻击模型 系统的安全取决于系统环境和攻击者的能力，称一个明确的环境和攻击能力假定的整体为一个攻击模型。下面给出现有的主要的确定攻击模型的参量或假设，以此描述攻击模型“线索”。

(1) 同步和异步：实际通信方式存在同步和异步信道之分，分布式密码设计时通常先考虑同步信道，然后结合异步信道特点考虑异步信道下的实现。

信息论信道和复杂性信道：对应攻击者的计算能力无限和有限假设，无限计算能力下，需要假设攻击者不能访问两两用户间通信信道和广播信道，称为信息论（安全）信道模型；而有限计算能力下，因假设存在如不可破译的密码等基本工具，可假设攻击者能够得到所有用户间通信消息和广播消息，称为复杂性（计算、密码）信道模型。

(2) 被动（Passive）攻击和主动（Active）攻击：如果攻击者在攻击中仅被动利用系统的公开通信消息和被拉拢用户的输入和接收信息，称为被动攻击；如攻击者进一步随意改变被拉拢用户的输入，则称为主动攻击。

(3) 静态（Static）攻击或非适应性（Non-Adptive）攻击和动态（Dynamic）攻击或适应性（Adptive）攻击：如攻击者在协议执行之初选定了拉拢用户集合且攻击过程中保持不变，称为静态攻击；而如果攻击者在攻击过程中可以在事先规定的范围内根据需要任意选择拉拢用户，则称为动态攻击。

动态攻击下有一类特殊的移动（Mobile）攻击，攻击者有较强的能力，可在相对较长时间内逐一攻破各个用户。对抗移动攻击的方式是系统在保持共享的秘密不变下定期对份额进行更新，此方式称为前置安全（Proactive security），也已是分布式密码研究的一项重要内容。

还有其他一些攻击模型参量，如动态攻击中考虑用户是否有能力随时安全删除自己不再使用的秘密信息，再如考虑在每一轮开始时，攻击者是否可以先得到诚实用户输出，然后据此确定拉拢某些新的用户或确定拉拢用户的输出（如能够则称为占先攻击）。随着应用环境的变化和研究的深入，新的参量或假设可能不断出现。

3 分布式密码的研究内容

安全是密码方案的首要要求，分布式密码也不例外。各种攻击模型下各类具体问题的模型描述和安全性定义是分布式密码的首要问题，目前基本上是通过对SMPC或多方安全协议研究中提出的模型和安全性定义进行具体化实现，与安全多方计算及协议一样，更好的模型描述和安全性定义是迫切需要的。

类似访问结构可定义攻击结构（Γ_A，Δ_A）[11]，其中P的子集B属于Γ_A表示B中成员全被拉拢。显然，首先仅当$\Gamma_A \cap \Gamma$为空集条件下，系统才能安全，这就需要对攻击者拉拢用户的能力进行一定限制，从而需要研究具体问题在各种攻击模型下安全方案存在的必要条件。

多数情况下，信息论模型下无条件安全的方案是不存在的，但如果建立起可有效实现的无条件安全方案，则认为对应问题得到了较好解决，即使不能得到有效构造，信息论模型在探讨一些理论问题002可能具有重要意义。目前计算模型下安全性的热点是安全性证明，利用归约思想将安全性与一些计算困难假设联系起来，论证可将有效的攻击算法转化为解计算困难假设问题的有效算法，以此证明体制的安全性。分布式密码的安全性证明主要是归约到对应的集中式密码的安全性，方法也是通用的所谓模拟器技术，即建立可以以计算不可区分分布模拟攻击者行为的模拟器[8]。安全性证明是一大难点。在安全性定义和必要条件下，具体构造分布式密码并证明安全性是挑战性的工作。

显然，主动攻击能力强于被动攻击，系统设计时经常是先设计抗击被动攻击的方案，然后通过某些加强手段去抗击主动攻击。主动攻击下主要是考虑系统的鲁棒性（Robustness），即在攻击下诚实用户依然可以完成预定的任务，如VSS正是为SS提供鲁棒性而设计的。从抗被动攻击到抗主动攻击的一般方法是对用户的输入进行一定“约束”以保持与系统设计一致，主要是对输入通过承诺或零知识证明进行某种有效性验证，其中可验证秘密共享起着重要作用。另外，将输入与某种纠错码相结合以对输入进行一定的检错纠错也是一条思路，但实现起来通常比较困难。

同样，动态攻击能力强于静态攻击，系统设计时经常是先设计抗击静态攻击的方案，然后通过某些加强手段去抗击动态攻击。实现从抗静态攻击到抗动态攻击理论和实践上都比较困难，虽然已经有一些成果，但仍是重点和难点。

可以有效实现是密码方案实用的前提，分布式密码通常是一个包含各种算法的复杂协议，在分析实现效率时，除了计算复杂度和存储（空间）复杂度外，必须同时考虑通信复杂度，其中包括消息复杂度和轮复杂度，分别考虑协议执行中发送消息和需要轮数的规模。另外，鉴于大量使用随机化算法，必须考虑随机化复杂度，即方案中使用的随机数或随机序列的规模。各种分布式密码实现效率的理论界可能可以理论分析出来，但通常较为困难，目前主要针对具体实现进

行估算，然后与实际实现能力、已有方案及可能的理论界进行比较来衡量效率。

现有分布式密码方案几乎都是基于秘密共享方案，核心在于实现秘密共享算法和密码算法的有机结合，这就要求两类算法都具有一定的所谓同态性。所以，安全高效且能与现有密码算法有效结合的秘密共享算法，是实现分布式密码的基础。门限条件下，Shamir 方案[1]既是完善的又是理想的，且具有很好的同态性，对秘密的运算可以通过对对应份额的适当运算实现，因而几乎是所有现有门限密码实现的基础。而一般访问结构下，秘密共享算法只有基于向量空间理论的算法，主要是基于 MSP(Monotone Span Program)的线性秘密共享算法[12]，但 MSP 的有效构造尚未解决，而且难于构建需要的同态性，对应分布式密码实现成果几乎没有。所以，当前分布式密码主要是门限密码。

门限密码目前集中在现有公钥体制的分布式实现上，包括基于离散对数问题的体制和 RSA 等，从鲁棒的到抗动态攻击的以及前置安全的都已经有一些成果[13]，但整体上效率都有待提高。实现时自然需要将密码算法中的各种基本运算分布式实现，所以，通过秘密共享算法分布式实现通常的运算成为分布式密码的基础性工作[14,15]。因为目前实用的共享算法只有加法（秘密是所有份额的和）和 Shamir 门限算法，所以实现分布式乘法是重点。另外，鉴于为解决 RSA 分布式实现已将 Shamir 算法由域推广到环上，沿此思路自然考虑群和环上运算的分布式实现[16,17]。

4　结论

本文给出了分布式密码的体系结构，比较清晰地描述了分布式密码的主要内容，同时，较为完整地描述了分布式密码的系统模型，最后对主要研究内容进行了简要介绍。

参 考 文 献

[1] Shamir A. How to share a secret[J]. *Communications of the* ACM, 1979, 22(11): 612 – 613.

[2] Blakley G R. Safeguarding cryptographic keys[C]. Proc. National Computer Conference'79, AFIPS Proceedings, 1979, vol.48: 313 – 317.

[3] Ito M, Saito A, Nishizeki T. Secret sharing scheme realizing general access structure[C]. IEEE Globcom'87, Tokyo Japan, 1987: 99 – 102.

[4] Desmedt Y. Society and group oriented cryptography: a new concept[C]. Proc. of CRYPTO'87, California USA, 1988: 120 – 127.

[5] Desmedt Y, Frankel Y. Threshold cryptosystems[C]. Proc. of CRYPTO'89, California USA, 1990: 307 – 315.

[6] Chor B, Goldwasser S, Micali S, Awerbuch B. Verifiable secret sharing and achieving simultaneity in the presence of faults[C]. Proc. of IEEE 26-th Annual Symp. on FOCS, Portland, Oregon, 1985: 383 – 395.

[7] Yao A C. Protocols for secure computations[C]. Proc. 23rd Ann. Symp. on Foundations of Computer Science, California USA, 1982: 160 – 164.

[8] Goldreich O. Secure Multi-party Computation. http:// www.wisdom.weizmann.ac.il~oded.

[9] Canetti R. Studies in secure multiparty computation and applications[D]. [Ph.D. thesis], Weizmann Institute of Science, 1995.

[10] Desmedt Y, Wang Y. Perfectly secure message transmission revisited[C]. Proc. of EUROCRYPT'02, Amsterdam, the Netherlands, 2002: 502 – 517.

[11] Hirt M, Maurer U. Player simulation and general adversary structures in perfect multiparty computation[J]. Journal of Cryptology, 2000, 13(1): 31 – 60.

[12] Karchmer K., Wigderson A. On span programs[C]. Proc. of 8-th Annual Structure in IEEE Complexity Theory Conference, 1993: 102 – 111.

[13] Stanislaw J. Efficient threshold cryptosystems[D]. [PH.D. thesis], MIT, 2001.

[14] Catalano D, Gennaro R, Halevi S. Computing inverses over a shared secret modulus[C]. Proc. of EUROCRYPT'02, Amsterdam, the Netherlands, 2002: 190 – 206.

[15] Algesheimer J, Camenisch J, Shoup V. Efficient computation modulo a shared secret with application to the generation of shared safe-prime products. http://eprint.iacr.org/2002 – 029.

[16] Cramer R, Fehr S. Optimal black-box secret sharing over arbitrary Abelian groups[C]. Proc. of CRYPTO'02, California, USA, 2002: 272 – 287.

[17] Cramer R, Fehr S, Ishai Y, Kushilevitz K. Efficient multi-party computation over rings[C]. Proc. of EUROCRYPT'03, Warsaw, Poland, 2003: 578 – 595.

王　磊：　男，1972 年生，博士生，研究方向为密码学.

祝跃飞：　男，1962 年生，教授，博士生导师，研究方向为密码学.