IKEにおける認証モードとサービス妨害攻撃耐性の解析

3F－5

松浦 幹太[1]
東京大学

1 はじめに

IPsec(IP security protocols) のワーキンググループにおいて ISAKMP/Oakley として策定作業が進められてきた鍵共有プロトコルが、1998 年 11 月に IKE(Internet Key Exchange) として RFC(Standards Track) 化された [1]。IKE の第一フェーズは、Diffie-Hellman 鍵共有プロトコル [2] に基づいている。リクエストを発するプロトコル参加者を始動者と呼び、それに応対する者を応答者と呼ぶ。中間一致攻撃対策のため認証機構が組み込まれているが、公開鍵を利用した方式では認証に要するコストがサービス妨害 (Denial-of-Service: DoS) 攻撃に悪用されかねない。すなわち、でたらめなリクエストに次々と襲われた場合、応答者は検証作業で計算機資源を使い果たし、サービス不能状態に陥る恐れがある。安全性のための認証が、かえって、サービス妨害を意図したリクエスト 1 個当たりのダメージを大きくしているわけである。これは、安全性と可用性のトレードオフとも言え、大きな問題である。

本稿では、まず第 2章で、IKE に対する代表的な DoS 攻撃とそれらへの対策をまとめる。次に、議論を IKE の Aggressive Mode に絞り、第 3章で DoS 対策の評価を行う。そこでは、(1) 認証モード毎の DoS 耐性の相違、(2)DoS 耐性の高い認証モードで DoS 対策を十分に機能させる最適化の効果、(3) 同モードにおける応答者側でのパケット棄却の効果について考察する。第 4章はまとめである。

2 サービス妨害攻撃と対策

2.1 攻撃

IKE では、DoS を考慮して簡易な Anti-Clogging Token である Cookie が使われている [3], [4]。しかし、それには弱点があり、Cookie Crumb Attack と Cookie Jar Attack が問題視されている [5]。

Cookie Crumb Attack は、でたらめなリクエストで Cookie 関連の状態を応答者のメモリーに多数蓄積させ、そのメモリー資源を枯渇させる攻撃である。これは Cookie がパスする以前の問題であり、プロトコルをどの程度 stateless に近づけられるかが対策のポイントとなる。

Cookie Jar Attack は、有効な Cookie を多数集めてから (Cookie チェックにパスする) リクエストを多数発し、署名検証作業等の公開鍵計算負荷で応答者の CPU をハングアップさせる攻撃である。これは再送攻撃の一種であり、再送できる個数を抑えることと、攻撃 1 個が与えるダメージ（応答者側にかかる計算負荷）を抑えることが対策のポイントとなる。

---

[1]DoS-Resistance Analysis of Authentication Modes in IKE
Kanta Matsuura
Institute of Industrial Science, the University of Tokyo
Roppongi 7-22-1, Minato-Ku, Tokyo 106-8558, JAPAN.

一方、IKE の拡張方式として、二段階の認証も検討されている [6]。そこでは、まず第一段階で始動者が応答者（サーバ）を公開鍵に基づいて認証する。逆の認証は第二段階で行われ、事前に共有したパラメータや長期の秘密情報も利用可能である。これは、鍵の更新や、第二段階でアプリケーションと直結した認証を行うことを意識している。第二段階の認証方式次第では、第一段階をパスした後で「ID は正しいけれども第二段階をパスできないリクエスト」を多数発し、サーバがその ID をブラックリストに載せるよう仕向ける User-Revokation Attack が可能である。これも (当該 ID のエンティティがサービスを利用できなくなるという意味で) DoS 攻撃の一種だが、本稿で耐性を考える対象ではない。

2.2 対策

Cookie Crumb Attack に関しては、

- Cookie 本来の stateless 要件 [4] を満たすよう、実装に制限を加える。
- stateless connection の考え方 [7]–[9] を応用し、状態を暗号化して送り、それをそのまま送り返させる。

等の対策がある。公開鍵系の認証をする IKE の Aggressive Mode(3 パスのプロトコル) に議論を絞れば、メモリー枯渇へもっとも影響する要素は Cookie 関連ではなく公開鍵系のパラメータであると見なせる。

Cookie Jar Attack に関しては、

1. 同一 IP アドレスと、同時に複数の IKE を実行しない。
2. Network Ingress Filtering[10] により、ローカルルータが外部へ向かうパケットの送信元アドレスをチェックし、自分の管轄外の不正な（または誤った）ものは破棄する。
3. 攻撃者にも応答者並の計算機資源消費を余儀なくさせる「共倒れ方式」[11] に基づいて、IKE の署名モードを改善する [12]。

等の対策がある。筆者らは、既に

- IKE は、認証モードとして（改善）署名モードを使用している。
- 対策 1と対策 2によって、極めて短時間に到来する攻撃の個数がある程度制限される。
- 対策 3によって、応答者（サーバ）がハングアップするか否かは、CPU ではなくメモリ枯渇で決定される。

という状況において、サーバ閉塞率を評価している [13]。本稿では、攻撃者が検査をパスする Cookie を十分多く持っていると仮定した上で、Cookie Jar Attack 対策の効果をより詳しく調べる。

具体的には、次章で、まず認証モードによる差異を指摘する。次に、対策 3を活用する最適化の効果を論じる。さらに、ランダムなパケット棄却がサーバ閉塞率にどう影響するかを評価する。

3 評価

3.1 認証モードによる差異

攻撃者を次の二種類に分類して考察する。

(タイプ 1) パケットフォーマットのように形式的なことは守るが、内容的にはまったくでたらめな Request と Acknowledgment しか送らない攻撃者。

(タイプ 2) 形式的なことを守るだけでなく、署名検証のように相手に依存した公開鍵オペレーションを応答者に行わせるため、最低限プロトコルにしたがう攻撃者。

不正なリクエスト 1 個がタイプ 1 の攻撃者・応答者それぞれの側に生じさせる計算負荷を「公開鍵オペレーションに要する法乗算の回数」で評価した結果を、表 1に示す。各アルゴリズムの安全性は、1024bit の RSA 合成数に相当するレベルを仮定した。攻撃 1 個が与えるダメージ（応答者側にかかる計算負荷）が抑えられているという意味で、改善署名モードが際立って CPU 枯渇に強いモードであることが分かる。

表 1: タイプ 1 の攻撃者の場合に不正なリクエスト 1 個が生じる計算負荷.

認証モード (アルゴリズム)	攻撃者側の負荷	応答者側の負荷
公開鍵暗号モード (RSA)	0	384
公開鍵暗号モード (ElGamal)	0	1536
改善公開鍵暗号モード (RSA)	0	384
改善公開鍵暗号モード (ElGamal)	0	1536
署名モード (RSA)	0	384
署名モード (ElGamal)	0	4608
署名モード (DSS)	0	480
署名モード (Schnorr)	0	480
改善署名モード (SDSS)	0	0
改善署名モード (Schnorr)	0	0

次に、タイプ 2 の攻撃者を想定して同様の評価を行った結果を、表 2に示す。改善署名モードでも応答者側に負荷が生じているが、その 58.3% の負荷が攻撃者側にも生じている。なお、少なくとも Diffie-Hellman 公開値をベキ乗しない分だけは、正当なリクエストを最後まで処理した時よりも応答者側に生じる負荷は少ない。

3.2 最適化の効果

改善署名モードで正当なリクエストを処理する負荷は、事前計算負荷 c_1、署名検証負荷 c_2、Diffie-Hellman 鍵生成負荷 c_3 から成る。文献 [13] のサーバ閉塞率評価では、応答者が不正なリクエストを処理する負荷と正当なリクエストを処理する負荷が同じであると仮定していた。実際には、実装最適化により、タイプ 1 の攻撃者の場合で$\gamma = c_1/(c_1 + c_2 + c_3) = 0.25$、タイプ 2 の攻撃者の場合で$\gamma = (c_1 + c_2)(c_1 + c_2 + c_3) = 0.75$ というコスト削減係数を達成できる可能性がある。ここでは、$0.25 \leq \gamma \leq 1.0$ の範囲で、最適化の効果を調べる。

表 2: タイプ 2 の攻撃者の場合に不正なリクエスト 1 個が生じる計算負荷.

認証モード (アルゴリズム)	攻撃者側の負荷	応答者側の負荷
公開鍵暗号モード (RSA)	0	384
公開鍵暗号モード (ElGamal)	0	1536
改善公開鍵暗号モード (RSA)	0	384
改善公開鍵暗号モード (ElGamal)	0	1536
署名モード (RSA)	0	384
署名モード (ElGamal)	0	4608
署名モード (DSS)	0	480
署名モード (Schnorr)	0	480
改善署名モード (SDSS)	280	480
改善署名モード (Schnorr)	280	480

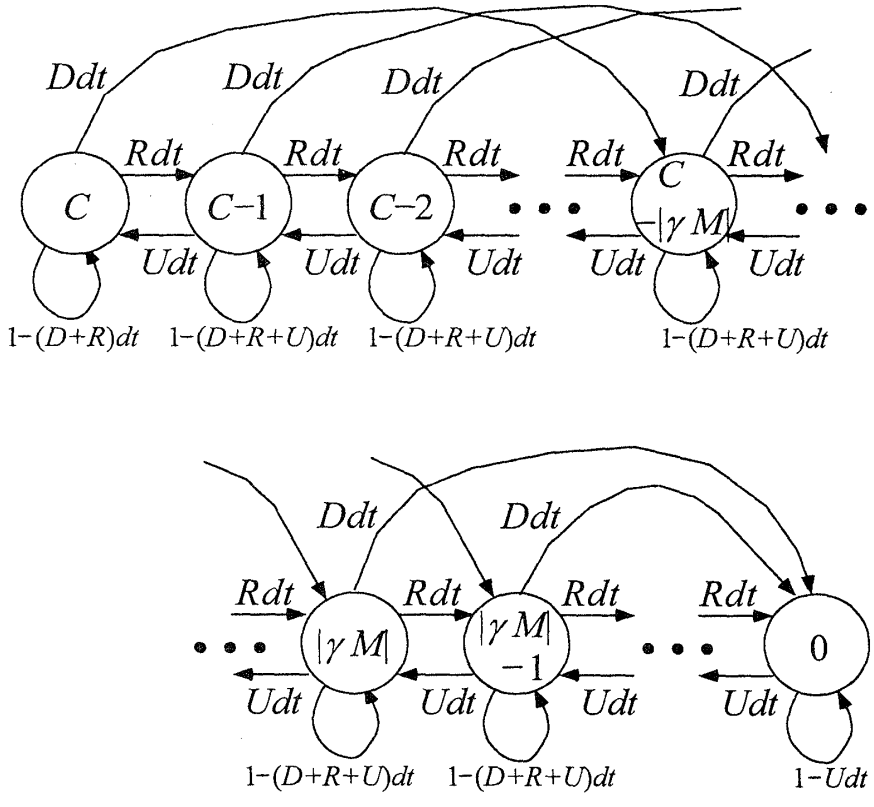


図 1: IKE の改善署名モードにおける応答者の状態遷移図. γはコスト削減係数.

具体的には、以下のように単純化したモデルを用いる。

1. 1回の攻撃で送りつけられる不正なリクエストの数は一定 (M個) である。これらは、$\lfloor \gamma M \rfloor \equiv$ (γMの小数点以下を四捨五入した整数) 個の正当なリクエストと同等の負荷を生じる。
2. 応答者が蓄えることのできる事前計算値は、C組までである。これを事前計算容量と呼ぶ。
3. 時域 $[t, t+dt]$ の間に1つのサービス妨害攻撃が到来する確率は dt に比例し、$D \cdot dt$ である。 D を攻撃生起率と呼ぶ。
4. 時域 $[t, t+dt]$ の間に正当なリクエストが到来する確率は dt に比例し、$R \cdot dt$ である。 R を要求生起率と呼ぶ。
5. 時域 $[t, t+dt]$ の間に新たな事前計算値を1組計算できる確率は dt に比例し、$U \cdot dt$ である。U を事前計算能率と呼ぶ。
6. システムは閉塞系であり、統計的平衡状態にある。

各状態を応答者が保持している事前計算値の組数で表せば、状態遷移図は図1のようになる。

$C = 1000$, $R = 0.001$, $M = 256$, $\gamma = 0.48$ とした時の閉塞率（状態0である確率）は図2のように評価される。たとえ攻撃生起率が0.1（毎分50000個から80000個程度の不正な要求に襲われる場合）であっても、閉塞率は10%に満たない。$0.25 \leq \gamma \leq 1.0$ の範囲でコスト削減係数を変えて評価しても、この性質は変わらない。図2(b)を見れば、攻撃生起率が閾値 $D_{th} \simeq 0.006$ を越えると、閉塞率が急激に上昇し始めることがわかる。$0.25 \leq \gamma \leq 1.0$ の範囲で評価すると、この閾値が変化する。その様子を図3に示す。

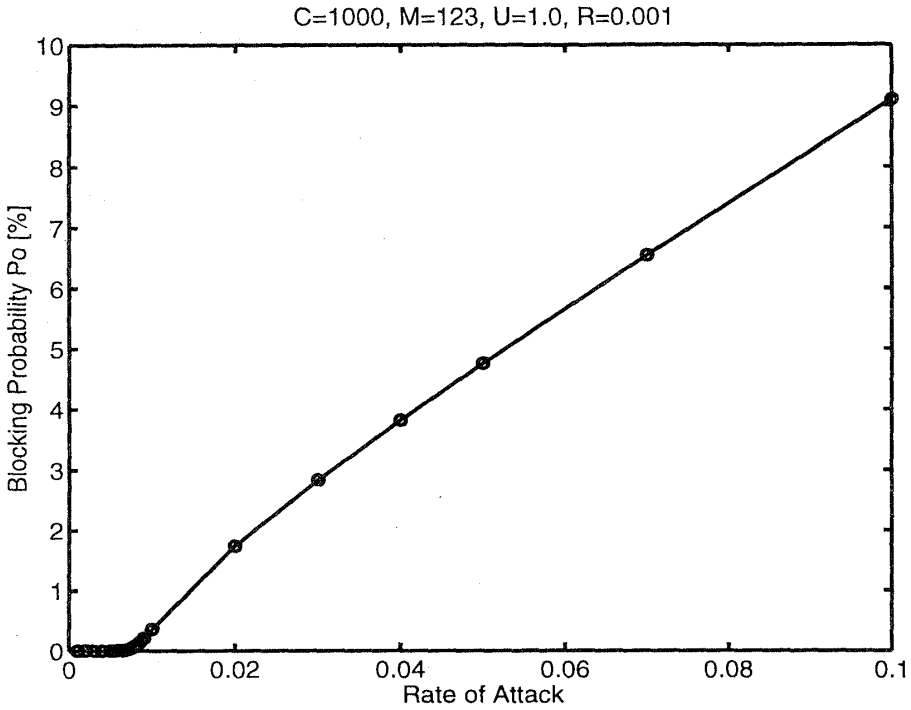
3.3 パケット棄却の効果

鍵共有プロトコルに依存しないDoS対策としては、正当か不正かに関わらず応答者側でランダムにリクエストを棄却するという方法も考えられる。その問題点の一つは、正当な利用者の利便性とのバランスをとるのが難しいことである。しかも、バランスをとる以前に、ランダム棄却の効果に関する定量的評価が不足している。本節では、図1のモデルを応用した定量的評価を報告する。

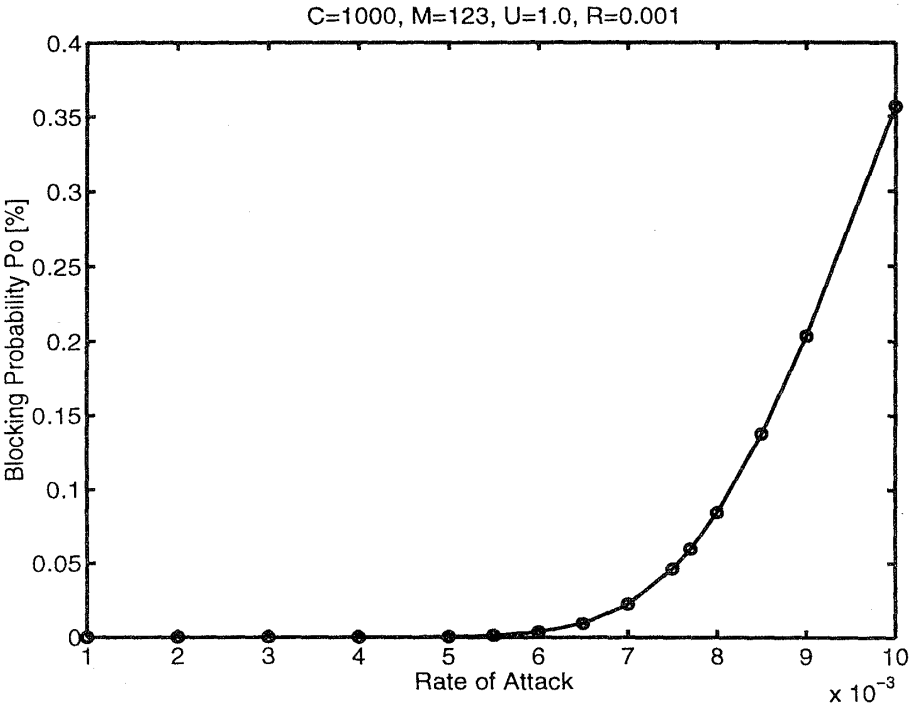
応答者側がランダムにリクエストを棄却する確率をα=1.0% とする。この時、図1における攻撃規模 Mを $(1-\alpha)M$で置き換え、要求生起率 Rを $(1-\alpha)R$で置き換えてサーバ閉塞率を求めた。その結果を図4に示す。図2と比べて、ほとんど特性が変化していないことがわかる。

4 むすび

IKEの第一フェーズでは、認証方式にいくつか異なるモードがある。それらをDoS攻撃耐性の観点で比較分析し、改善署名モードが優れていることを示した。これによりメモリ枯渇で閉塞を判断できるようになれば、定量的なDoS耐性評価が容易になる。実際に数百KB程度のメモリを仮定して評価した結果、毎分50000個から80000個程度の不正な要求に襲われる場合であっても閉塞率は10%に満たないことを確認した。さらに、DoS対策の最適化により閉塞率が急激に上昇し始める攻撃生起率閾値が改善されることと、ランダムなパケット棄却の効果がほとんどないことを明らかにした。今後は、メモリ枯渇対策の解析や、閉塞に至る前の中間的な状態におけるパフォーマンス低下の問題も考察したい。



(a) $D \leq 0.1$



(b) $D \leq 0.01$ の部分の拡大図

図 2: 事前計算容量 C=1000, コスト削減係数γ=0.48 である場合の閉塞率特性.

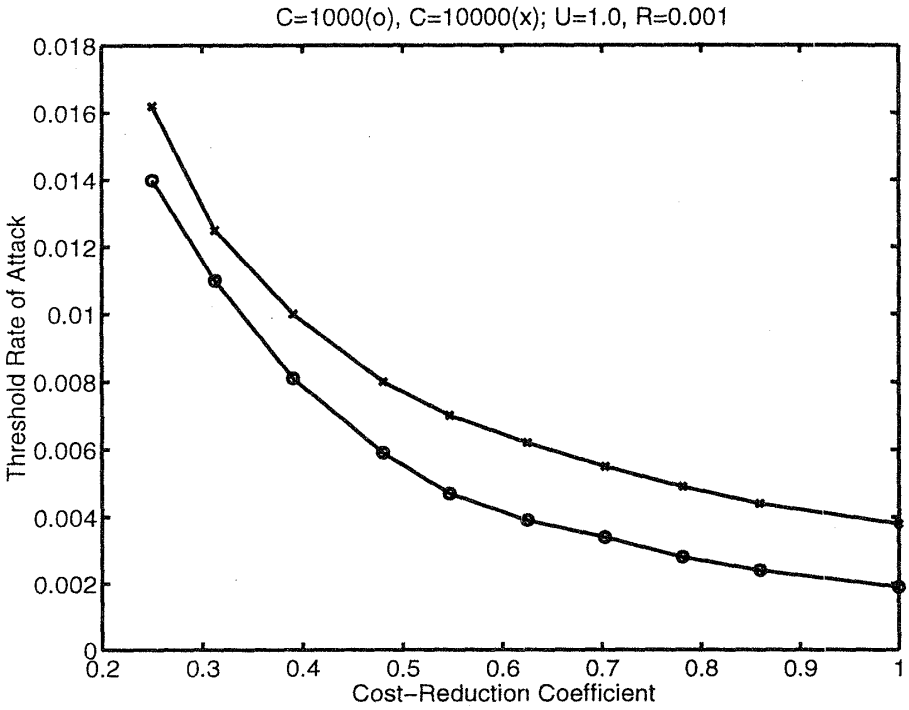


図 3: 最適化でコスト削減係数γが 1.0 から 0.25 まで変化した時の効果. 縦軸は攻撃生起率の閾値 D_{th}.

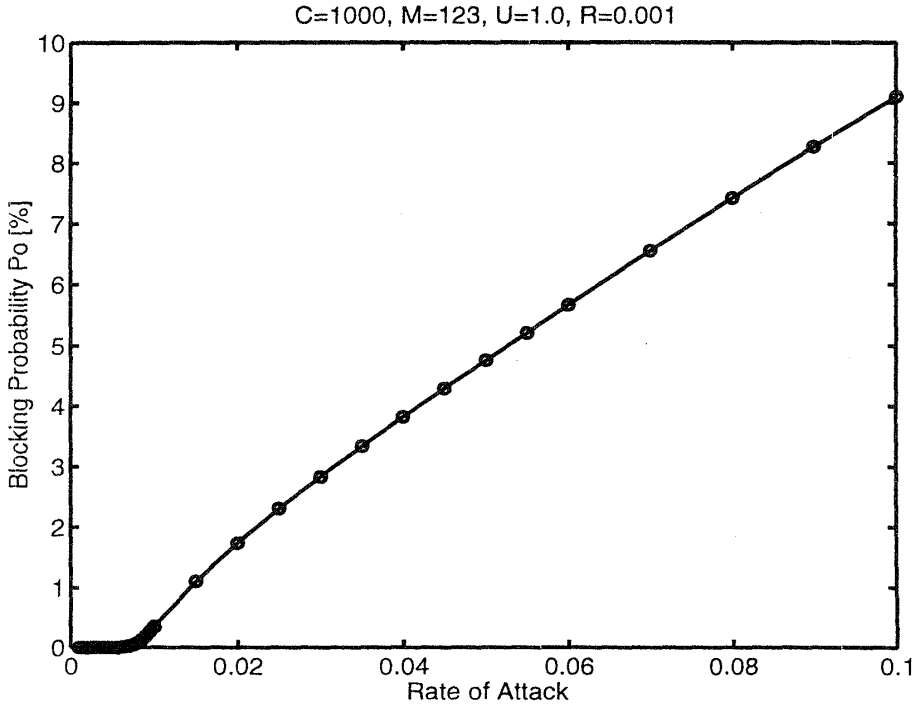


図 4: 事前計算容量 C=1000, コスト削減係数γ=0.48, ランダム棄却率α=0.01 である場合の閉塞率特性.

参考文献

[1] D. Harkins and D. Carrel. "The Internet Key Exchange (IKE)". rfc2409, November 1998.

[2] W. Diffie and M. Hellman. "New Directions in Cryptography". *IEEE Trans. Information Theory*, Vol. IT-22, No. 6, pp. 644–654, 1976.

[3] D. Maughan, M. Schertler, M. Schneider, and J. Turner. "Internet Security Association and Key Management Protocol (ISAKMP)". rfc2408, November 1998.

[4] P. Karn and W. Simpson. "Photuris: Session-Key Management Protocol". rfc2522, March 1999.

[5] W. A. Simpson. "IKE/ISAKMP Considered Dangerous". draft-simpson-danger-isakmp-**.txt (Work in progress)

[6] R. Pereira and S. Beaulieu. "Extended Authentication within ISAKMP/Oakley". draft-ietf-ipsec-isakmp-xauth-**.txt (Work in progress)

[7] T. Aura and P. Nikander. "Stateless Connections". In *Information and Communications Security*, Lecture Notes in Computer Science 1334, pp. 87–97, 1997. Springer-Verlag.

[8] 廣瀬勝一, 松浦幹太. "サービス拒否攻撃に対して耐性のある鍵共有プロトコル". 電子情報通信学会 1998 年基礎・境界ソサイエティ大会, October 1998.

[9] S. Hirose and K. Matsuura. "Enhancing the Resistance of a Secure Key Agreement Protocol to a Denial-of-Service Attack". In *Proc. of the 1999 Symposium on Cryptography and Information Security (SCIS'99)*, Vol. II, pp. 899–904, January 1999.

[10] P. Ferguson and D. Senie. "Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing". rfc2267, January 1998.

[11] K. Matsuura and H. Imai. "Protection of Authenticated Key-Agreement Protocol against a Denial-of-Service Attack". *Proceedings of 1998 International Symposium on Information Theory and Its Applications (ISITA'98)*, pp. 466–470, October 1998.

[12] K. Matsuura and H. Imai. "Resolution of ISAKMP/Oakley Key-Agreement Protocol Resistant against Denial-of-Service Attack". In *Pre-Proc. of Internet Workshop'99 (IWS'99)*, pp. 17–24, February 1999.

[13] 松浦幹太, 今井秀樹. "発信フィルタリング環境下の鍵共有プロトコルにおける閉塞率評価". 1999 年暗号と情報セキュリティ・シンポジウム (SCIS'99) 予稿集, Vol. II, pp. 893–898, 1999.