組込み機器に秘密共有機能を提供する SIM カード型セキュアチップの開発

宮崎 真悟† 石川 千秋† 鵜坂 智則‡ 小俣 三郎† 越塚 登† 坂村 健†
†YRP ユビキタス・ネットワーキング研究所
‡東京大学総合研究博物館

1 はじめに

近年，情報のセキュリティが重要視される中，インターネットといった公衆網に暗号技術で保護された仮想的な専用通信路を確立する VPN (Virtual Private Network) 技術が普及している．その主な通信ノードは，パーソナルコンピュータや専用ルータ，エンタプライズサーバといった豊富な計算資源を具備した機器である．

一方で，現在急速に研究開発が進められているユビキタスコンピューティング環境では，生活空間の至る所に大小機能様々な組込み機器が浸透し，それらが様々な通信網を介して生活に関わる情報を相互にやり取りする．こうした様々な組込み機器のデータ通信にも上記 VPN のようなセキュリティ保護が重要となる．

計算資源に厳しい実装制約のある組込み機器でも小型実装や高速処理が可能な暗号認証処理を行うには，その礎となる相手ノードとの秘密の共有情報が必要である．この秘密共有に関しては公開鍵暗号技術が有効であるが，その計算量，固定的な鍵情報の厳重管理が問題となる．

この課題への解を，汎用セキュリティアーキテクチャである eTRON[2, 4] の上で実現した研究開発事例は従来にはない．eTRON は，ユビキタスコンピューティングに対する世界規模の標準開発環境 T-Engine[5] にて，標準のセキュリティアーキテクチャとなっている．

我々は，秘密共有に必要な演算処理や鍵情報管理の一切を担い，対象機器に外部から秘密共有機能を提供する SIM カード型 eTRON/16 チップを開発した．本稿では，本開発チップの概要と組込みシステムへの応用を示す．

2 開発チップの概要

2.1 設計要件

本開発チップの設計要件は，以下のとおりである．

- **MTI/A0 方式 [3] に基づく秘密共有機能：**接続した組込み機器を介して，相手ノードと秘密共有に必要な情報を交換する．その交換情報の正当性を検証の上，内部で生成した秘密擬似乱数と自身のプライベート鍵とを用いて秘密共有情報を計算，接続機器へ出力する．
- **通信網の汎用性：** 接続する機器と相手機器間の通信網は規定しない．インターネット，モバイル網，無線 LAN，Bluetooth，赤外線通信といった接続機器で対応可能な様々な通信網を設定できる．
- **接続機器との暗号認証通信：** 組込み機器と開発チップ間の通信は eTRON の通信規約に従い，その通信データを暗号技術で保護する．

図 1: 開発した SIM カード型 eTRON/16 チップ

2.2 開発チップの特徴

16 ビットのマイクロコントローラを搭載した本開発チップは，以下の特徴を有している（図 1 参照）．

- **ISO/IEC 7816 準拠の物理インタフェース：**組込み機器との接触型通信．
- **暗号コプロセッサ：** 秘密共有処理に必要な公開鍵暗号系の剰余演算を高速処理．
- **耐タンパ性：** チップ内部の制御プログラムや格納情報をセキュリティ保護．
- **SIM カード形状：** その可搬性により，特定機器に限らず，異なる複数の機器への着脱使用が可能．

組込み機器への接続例として，ユビキタスコンピューティング環境との会話を行うユビキタスコミュニケータ [5]，設備機器や家電機器の制御を行う nT-Engine[5] への適用をそれぞれ図 2 と図 3 に示す．

3 開発チップの秘密共有機能とその応用

応用例として，本開発チップの秘密共有機能を用いた，組込み機器の暗号認証通信を例示する．今，組込み機器 P および Q が，本チップを用いて，当該機器間

"Development of SIM card formed security chips for supporting a secret sharing between embedded devices," by Shingo MIYAZAKI†, Chiaki ISHIKAWA†, Tomonori USAKA‡, Saburo OMATA†, Noboru KOSHIZUKA†, and Ken SAKAMURA†
† YRP Ubiquitous Networking Laboratory
‡ The University Museum, The University of Tokyo

図 2: ユビキタスコミュニケータへの接続

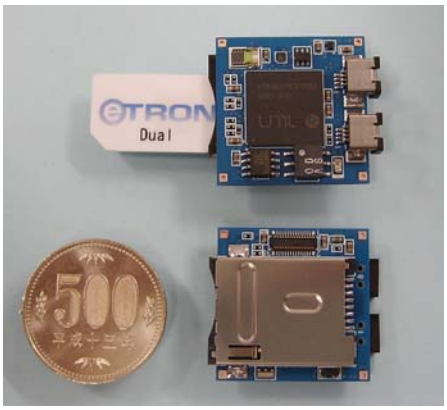

図 3: nT-Engine への接続

の暗号認証通信に必要な暗号鍵を秘密共有する場合を考える．その基本的な流れを以下に示す（図 4 参照）．

Step.1: 組込み機器 P および Q は，それぞれ接続したセキュアチップに対して秘密共有要求を行う．

Step.2: セキュアチップ A および B は，内部生成した秘密擬似乱数で冪乗剰余値（以下，コミット値）を計算し，自身の公開鍵証明書と共に接続機器へ送信する．

Step.3: 組込み機器 P および Q は，その間の通信網で定められた通信規約に従い，接続チップからの公開鍵証明書とコミット値を相互に交換する．さらに eTRON の通信規約に従い，相手機器から受信した公開鍵証明書とコミット値を接続チップに送信する．

Step.4: セキュアチップ A および B は，受信した公開鍵証明書の正当性を検証する．正当な場合に限り，**Step.1** で内部生成した秘密擬似乱数，自身のプライベート鍵，受信したコミット値および公開鍵から共有秘密情報 K* を計算し，接続機器へ出力する．

Step.5: 組込み機器 P および Q は，共有秘密情報 K を用いた高速な暗号認証通信を行う．

*チップ A とチップ B とで生成される K は同値となる．

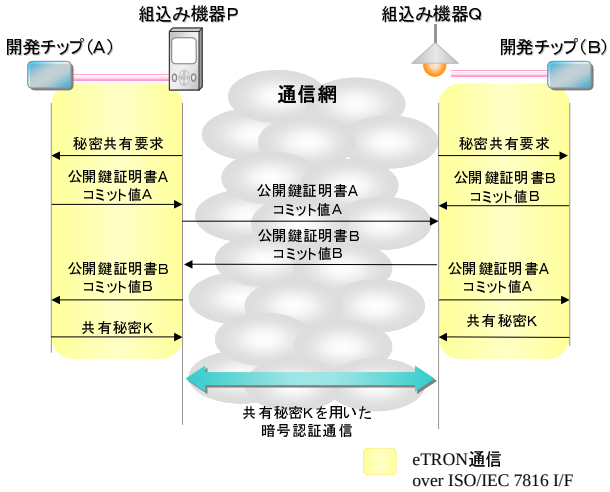

図 4: 開発チップを用いた組込み機器間の暗号鍵共有

本開発チップが提供する秘密共有情報は，単に相手ノードとの暗号鍵としてだけでなく，各種の権限情報として利用してもよい．例えば，同秘密情報を基に少額決済用の電子現金や電子クーポン，アクセス認証チケットを生成するといった幅広い応用が可能である．

4 まとめ

本稿では，開発した SIM カード型セキュアチップの概要と組込みシステムへの応用を示した．主に組込み機器へのセキュリティ支援を記述したが，パーソナルコンピュータやエンタプライズサーバといった豊富な計算資源を具備する機器にも適用は可能である．特に，堅牢な耐タンパ性で保護されたセキュリティ情報および秘密共有情報の演算処理には，その利用価値がある．このように，特定の機器や通信網に依らない汎用性により，本開発チップの幅広い応用を期待できる．

参考文献

[1] W. Diffie and M. E. Hellman, “New Directions in Cryptography,” IEEE Transactions on Information Theory, IT-22, 6, pp. 644-654, 1976.

[2] 越塚 登, 坂村 健, “eTRON: Entity and Economy TRON,” 第 19 回情報処理学会コンピュータセキュリティ研究会, pp. 61-66, 2002 年 12 月.

[3] T. Matsumoto, Y. Takashima and H. Imai, “On seeking smart public-key distribution systems,” Transactions of the IEICE, Vol. 69, No. 2, pp. 99-106, 1986.

[4] K. Sakamura and N. Koshizuka, “The eTRON wide-area distributed-system architecture for E-Commerce,” IEEE Micro, Vol. 21, No. 6, pp.7-12, Dec. 2001.

[5] T-Engine Forum, `http://www.t-engine.org/`